UNIVERZITET U SARAJEVU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

SOCIJALNI INŽENJERING KAO PRIJETNJA SIGURNOSTI INFORMACIONIH SISTEMA

Sarajevo, novembar 2023. NATAŠA LIZDEK

POSVETA I ZAHVALNICA

S ponosom i neizmjernom ljubavlju posvećujem ovaj master rad mom dragom bratu Ognjenu (1988-2009).

Želim iskoristiti ovu priliku i da se iskreno zahvalim svima koji su mi pružili podršku tokom izrade ovog rada.

Najprije i najviše se zahvaljujem mojim roditeljima, ocu Miladinu i majci Mileni, na svesrdnoj roditeljskoj podršci koju su mi pružali tokom mog cjelokupnog obrazovanja, što su uvijek vjerovali u mene i podsticali me da sebi postavljam dovoljno visoke, a dostižne ciljeve. Sestri Tijani, na tome što je nepresušan izvor optimizma kojim me uvijek motiviše. Mom suprugu Borku, na strpljenju i ljubavi pruženim tokom studija i stvaranja ovog rada.

Posebno se zahvaljujem izvanrednoj mentorki, prof. dr Amri Kapo, koja me usmjeravala i bez suvišnih riječi znala jasno da me uputi na sljedeći korak prilikom izrade rada, na njenoj brzini i nesebičnoj podršci. Njena stručnost, strpljenje i posvećenost bili su ključni za uspješnu izradu ovog rada.

Takođe se zahvaljujem i mojim dragim profesorima, od kojih sam učila i učim, a koji su mi pružili moralnu i stručnu podršku tokom izrade rada, prof. dr Emini Resić, prof. dr Savi Stuparu i prof. dr Lazaru Radovanoviću, te mnogobrojnim drugim kolegama i prijateljima koji su me inspirisali da istrajem u svom istraživanju i razvoju.

Zahvaljujem se članovima komisije za ocjenu i odbranu završnog rada, prof. dr Kemalu Kačaporu i prof. dr Lejli Turulji na izdvojenom vremenu i trudu da pažljivo pregledaju i ocijene ovaj rad.

Na kraju, mada je neuobičajeno, ali ipak važno, zahvaljujem se nekadašnjoj sebi, koja je radila juče za bolje danas i sutra.

U skladu sa članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalistički studij na Univerzitetu u Sarajevu, daje se

IZJAVA O AUTENTIČNOSTI RADA

Ja, Nataša Lizdek, studentica drugog (II) ciklusa studija, broj indeksa 5511 na programu Master program u saradnji sa Microsoftom "MA+1", smjer Menadžment i informacioni sistemi, izjavljujem da sam završni rad na temu:

SOCIJALNI INŽENJERING KAO PRIJETNJA SIGURNOSTI INFORMACIONIH SISTEMA

pod mentorstvom prof. dr Amre Kapo izradila samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Rad ne sadrži prethodno objavljene ili neobjavljene materijale drugih autora, osim onih koji su priznati navođenjem literature i drugih izvora informacija uključujući i alate umjetne inteligencije.

Ovom izjavom potvrđujem da sam za potrebe arhiviranja predala elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija (ime, prezime, datum i mjesto rođenja, datum odbrane rada, naslov rada) na web stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu sa članom 34. 45. i 46. Zakona o autorskom i srodnim pravima (Službeni glasnik BiH, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, 10. 11. 2023. Potpis studentice:

SAŽETAK

Čovjek je najranjivija karika u lancu informacione sigurnosti, a socijalni inženjering je jedna od najznačajnijih prijetnji za sigurnost informacionih sistema. Prepoznajući ovu činjenicu, prva četiri istraživačka cilja završnog rada podrazumijevaju izlaganje osnovnih teorijskih postulata u vezi sa socijalnim inženjeringom kao prijetnji za sigurnost informacionih sistema (definicija pojma), objašnjenje različitih vrsta, a zatim i faza napada socijalnim inženjeringom, te načina odbrane od napada socijalnim inženjeringom. Peti istraživački cilj je da se izvrši analiza percepcije i zaštitnog ponašanja korisnika informacionih tehnologija u Bosni i Hercegovini prema prijetnjama od napada socijalnim inženjeringom na informacionu sigurnost. Metodologija istraživanja u ovom radu podrazumijeva kombinovanje pregleda već postojeće literature i sprovođenje empirijskog istraživanja. Pristup empirijskom istraživanju je kvantitativni - sastoji se od prikupljanja podataka kroz sprovođenje online ankete, analize podataka, te interpretacije rezultata i donošenja zaključka. Primarna kvantitativna istraživačka metoda korištena u radu je strukturalno modeliranje jednačina (eng. *Structural Equation Modeling, SEM*). Temeljni teoretski okvir za postavljanje hipoteza proizašao je iz Teorije motivacije za zaštitu (eng. *Protection Motivation Theory, PMT*). Posmatrano je šest latentnih konstrukata: percipirana ozbiljnost gubitaka, percipirana ranjivost, strah, motivacija za zaštitu, zaštitno ponašanje i obuka zaposlenih. Za donošenje odluke o statističkoj značajnosti veza među konstruktima korišteni su relevantni statistički pokazatelji, t-statistika i p-vrijednost. Potvrđene hipoteze pokazuju da percepcija ozbiljnosti mogućih gubitaka i ranjivosti korisnika statistički značajno pozitivno utiču na strah korisnika od napada socijalnim inženjeringom (H1 i H2). Takođe je utvrđeno da percipirana ozbiljnost potencijalnih gubitaka ima statistički značajnu ulogu u motivaciji korisnika za zaštitu od napada socijalnim inženjeringom (H4). Osim toga, motivacija korisnika za zaštitu od napada socijalnim inženjeringom pokazala se kao statistički značajan faktor koji pozitivno utiče na zaštitno ponašanje ispitanika (H6). Nadalje, potvrđeno je da sprovođenje obuke zaposlenih o sigurnosnim procedurama ima statistički značajan pozitivan uticaj na njihovo zaštitno ponašanje (H7). S druge strane, hipoteze H3 i H5 nisu prihvaćene jer analiza podataka nije otkrila statistički značajne korelacije između straha korisnika od napada socijalnim inženjeringom i njihove motivacije za zaštitu od napada, niti između percipirane ranjivosti korisnika i njihove motivacije za zaštitu. Potencijalno ograničenje sprovedenog empirijskog istraživanja ogleda se u tome što u obzir uzima subjektivne stavove ispitanika, odnosno anketa ne simulira stvarni strah koji bi ispitanici doživjeli da zaista postanu žrtva napada socijalnim inženjeringa. Uprkos navedenim ograničenjima, sprovedena anketa pokazala se kao validan izvor podataka za testiranje postavljenih hipoteza. Najzad, rad naglašava važnost kontinuirane edukacije i podizanja svijesti korisnika informacionih sistema. Nijedan informacioni sistem nikada ne može biti apsolutno (stopostotno) siguran, ali će biti bliži tom idealu ako se u obzir uzme i ljudski faktor kao ključna karika za uspješno očuvanje informacione sigurnosti.

ABSTRACT

Human beings represent the most vulnerable link in the chain of information security, while social engineering represents one of the most significant threats to the security of information systems. Recognizing this fact, the first four research objectives of the thesis involve presenting the fundamental theoretical tenets concerning social engineering as a threat to information systems security (including the definition of the concept), defining various types and phases of social engineering attacks, as well as the methods of defense against such attacks. The fifth research objective aims to analyze the perception and protective behavior of information technology users in Bosnia and Herzegovina concerning threats posed by social engineering to information security. The research methodology in this study entails a combination of reviewing existing literature and conducting empirical research. The empirical research approach is quantitative, involving data collection through an online survey, data analysis, interpretation of results, and drawing conclusions. The primary quantitative research method used in this study is Structural Equation Modeling (SEM). The foundational theoretical framework for hypothesis formulation is the Protection Motivation Theory (PMT). Six latent constructs were examined: perceived severity of losses, perceived vulnerability, fear, protection motivation, protective behavior, and employee training. Relevant statistical indicators, t-statistics and p-values, were utilized to determine the statistical significance of the relationships among these constructs. The confirmed hypotheses indicate that the perception of the severity of potential losses and user vulnerability significantly and positively influences users' fear of social engineering attacks (H1 and H2). Additionally, it was found that the perceived severity of potential losses plays a statistically significant role in motivating users to protect themselves against social engineering attacks (H4). Furthermore, users' motivation for protection against social engineering attacks has been identified as a statistically significant factor positively impacting their protective behavior (H6). Moreover, the hypothesis that employee training on security procedures has a statistically significant positive influence on their protective behavior was confirmed (H7). On the other hand, hypotheses H3 and H5 were not accepted as the data analysis did not reveal statistically significant correlations between users' fear of social engineering attacks and their motivation for protection or between users' perceived vulnerability and their motivation for protection. A potential limitation of the conducted empirical research is that it considers participants' subjective attitudes toward social engineering. In other words, the survey does not simulate the actual fear that participants would experience if they were to become victims of a social engineering attack. Despite these limitations, the conducted survey has proven to be a valid source of data for testing the formulated hypotheses. Lastly, the study emphasizes the importance of continuous education and raising awareness among information system users. No information system can ever be absolutely secure, but it will come closer to that ideal if the human factor is considered as a key element in successfully maintaining information security.

SADRŽAJ

1. UVOD 1

1.1. Obrazloženje teme i predmet istraživanja 1

1.2. Ciljevi istraživanja 2

1.3. Istraživačka pitanja 3

1.4. Hipoteze u istraživanju 3

1.5. Metodologija istraživanja 6

1.6. Struktura završnog rada 8

2. TEORETSKI OKVIR 9

2.1. Informaciona sigurnost 9

2.1.1. Definicija pojma informaciona sigurnost 9

2.1.2. Prijetnje informacionoj sigurnosti 11

2.2. Socijalni inženjering 12

2.2.1. Definicija pojma socijalni inženjering 12

2.2.2. Vrste napada socijalnim inženjeringom 15

2.2.2.1. Phishing 15

2.2.2.2. Baiting 16

2.2.2.3. Pretexting 16

2.2.2.4. Scareware 17

2.2.2.5. Dumpster diving 18

2.2.2.6. Obrnuti socijalni inženjering 19

2.2.2.7. Druge vrste socijalnog inženjeringa 19

2.2.3. Faze napada socijalnim inženjeringom 21

2.2.4. Načini odbrane od napada socijalnim inženjeringom 24

2.2.5. Teorija motivacije za zaštitu (eng. *Protection Motivation Theory, PMT*) 36

3. METODOLOGIJA I REZULTATI EMPIRIJSKOG ISTRAŽIVANJA 38

3.1. Metodologija empirijskog istraživanja 38

3.1.1. Strukturalno modeliranje jednačina (SEM) 38

3.1.2. Proces prikupljanja podataka 39

3.1.3. Opis uzorka 40

3.2. Rezultati i interpretacija rezultata empirijskog istraživanja 47

3.3. Ograničenja sprovedenog istraživanja 52

4. ZAKLJUČAK 52

REFERENCE 56

PRILOZI 61

POPIS TABELA

Tabela 1. Polna struktura ispitanika 41
Tabela 2. Obrazovna struktura ispitanika 41
Tabela 3. Industrija u kojoj su zaposleni ispitanici 42
Tabela 4. Starosna struktura ispitanika 43
Tabela 5. Hijerarhijska pozicija ispitanika u kompanijama 44
Tabela 6. Iskustvo ispitanika u korištenju računara (u godinama) 45
Tabela 7. Dosadašnja izloženost ispitanika napadima socijalnim inženjeringom 46
Tabela 8. Koeficijenti putanja 48
Tabela 9. T-statistika i p-vrijednost 49
Tabela 10. Sažetak rezultata testiranja hipoteza 49
Tabela 11. Koeficijent determinacije 50
Tabela 12. Vrijednost F^2 51
Tabela 13. Vrijednost Q^2 51

POPIS SLIKA

Dijagram 1. Predloženi istraživački model 8
Grafikon 1. Polna struktura ispitanika 41
Grafikon 2. Obrazovna struktura ispitanika 42
Grafikon 3. Industrija u kojoj su zaposleni ispitanici 43
Grafikon 4. Starosna struktura ispitanika 44
Grafikon 5. Hijerarhijska pozicija ispitanika u kompanijama 45
Grafikon 6. Iskustvo ispitanika u korištenju računara (u godinama) 46
Grafikon 7. Dosadašnja izloženost ispitanika napadima socijalnim inženjeringom 47

POPIS PRILOGA

Prilog 1. Anketa korištena u istraživanju 1

POPIS SKRAĆENICA

APWG – Anti-Phishing Working Group (Radna grupa za borbu protiv *phishing*-a, međunarodni konzorcijum)

C.I.A – Confidentiality, integrity and availabilty (povjerljivost, integritet i dostupnost, tri ključna elementa informacione sigurnosti)

CNSS – National Security Agency's Committee on National Security Systems (Komitet za sisteme nacionalne bezbjednosti Agencije za nacionalnu bezbjednost Sjedinjenih Američkih Država)

GDPR – General Data Protection Regulation (Opšta uredba o zaštiti podataka u Evropskoj uniji)

GUI – Graphical User Interface (grafički korisnički interfejs)

IDPS – Intrusion Detection and Prevention System (Sistem za detekciju i prevenciju upada)

IP – Internet protokol

ISO 27001 – International Organization for Standardization, International Standard for Information Security (međunarodni standard za informacionu sigurnost Međunarodne organizacije za standardizaciju)

ISP – Information Security Policies (politike informacione sigurnosti)

NIST – National Institute of Standards and Technology (Nacionalni institut za standarde i tehnologiju u Sjedinjenim Američkim Državama)

PDA – Personal Digital Assistant (lični digitalni pomoćnik, prenosni uređaj)

PLS – Partial Least Squares (metoda djelimičnih najmanjih kvadrata)

PMT – Protection Motivation Theory (teorija motivacije za zaštitu)

SEM – Structural Equation Modeling (strukturalno modeliranje jednačina)

SETA – Security Education Training Awareness (edukacija, trening i jačanje svijesti o informacionoj sigurnosti)

SSPA – Supplier Security and Privacy Assurance Program (program za osiguranje sigurnosti i privatnosti dobavljača)

URL – Uniform Resource Locator (web adresa)

USB – Universal Serial Bus (medijum za skladištenje digitalnih podataka)

VPN – Virtual Private Network (virtuelna privatna mreža)

1. UVOD

1.1. Obrazloženje teme i predmet istraživanja

Predmet istraživanja ovog master rada je socijalni inženjering kao potencijalna sigurnosna prijetnja za informacione sisteme. Svrha rada je da pojasni i istraži kako napadači koriste taktike socijalnog inženjeringa da bi dobili neovlašteni pristup povjerljivim informacijama i sistemima, koje faze čine jedan napad, te koje mjere sigurnosti se najčešće primjenjuju kako bi se izbjegla šteta od ovih napada. U empirijskom dijelu istraživanja sprovedena je anketa na reprezentativnom uzorku građana Bosne i Hercegovine o njihovoj percepciji i zaštitnom ponašanju u odnosu na socijalni inženjering. Zajedno sa datim teorijskim okvirom, sprovedeno empirijsko istraživanje čini srž naučnog doprinosa ovog rada postojećem znanju i razumijevanju socijalnog inženjeringa kao prijetnje informacionoj sigurnosti, naročito u specifičnom kontekstu Bosne i Hercegovine kao posmatranog područja.

Informaciona sigurnost je stanje, ali i proces očuvanja povjerljvosti, integriteta i dostupnosti digitalnih podataka. Da bi se postigli ovi ciljevi, potrebna je kombinacija alata, tehnologija za upravljanje rizicima, metodologija obuke i drugih specifičnih aktivnosti (Alsharif *et al*., 2022).

Prijetnje sigurnosti informacionih sistema eksploatišu ranjivosti sistema koje postoje, što povećava sigurnosne rizike. Jedna od glavnih prijetnji i najrasprostranjenijih i najuspješnijih vrsta napada na sigurnost informacionih sistema su napadi socijalnim inženjeringom (Duarte *et al*., 2021).

Socijalni inženjering je postupak manipulisanja korisnikom kako bi on obezbijedio određene informacije ili preduzeo određene aktivnosti kojima se ugrožava informaciona sigurnost (Patel, 2021). Odnosno, socijalni inženjering je tehnika kojom se manipuliše ljudima tako da oni svjesno ili nesvjesno omoguće pristup informacionom sistemu napadaču koji nije autorizovan da mu pristupi (Hadnagy, 2010).

Uspješan socijalni inženjering ima duboko negativan učinak na poslovanje - dovodi do gubitka podataka, finansijskih gubitaka, smanjenja morala zaposlenih i smanjene lojalnosti potrošača. U nekim okolnostima čak može doći do problema sa zakonskom i regulatornom usklađenošću organizacije, te izazvati sankcije i gubitke koji mogu proizaći iz kršenja pravnih propisa (Saxena *et al*., 2020).

Prijetnja koju predstavlja socijalni inženjering je univerzalna zbog neizbježnog postajanja ljudskih slabosti u pogledu njihovog odnosa prema informacionoj sigurnosti (Wang *et al*., 2020). Bez obzira na to koliko dobro su razvijene i implementirane mjere sigurnosti, ne postoji računarski sistem na svijetu koji u krajnjoj liniji ne zavisi od ponašanja ljudi. Ljudi kao faktor informacione sigurnosti ne samo da su podložni potpadanju pod uticaj socijalnog inženjeringa, već često predstavljaju najznačajniju slabu tačku, odnosno ranjivost informacionih sistema u poređenju sa svim ostalim ranjivostima informacionih sistema

(Wang *et al*., 2020). Meta napada mogu biti pojedinci, grupe pojedinaca ili organizacije (Mouton *et al*., 2016).

Samo jedna ljudska greška je dovoljna da neko postane žrtva napada socijalnim inženjeringom. Napadači često primjenjuju tehniku socijalnog inženjeringa jer je jednostavnije koristiti ljude kao objekat zloupotrebe, nego izdvojiti vrijeme i steći naprednije vještine potrebne za pronalaženje ranjivosti tehničke prirode u informacionim sistemima (Jones, 2022).

Salahdine i Kaabouch (2019) sumiraju da postoji dvadeset različitih vrsta napada socijalnim inženjeringom: *phishing*, korištenje mamca (eng. *baiting*), *pretexting, ransomware,* gledanje preko ramena, obrnuti socijalni inženjering, korištenje lažnog softvera, lažno predstavljanje na pozivima službi za pomoć, *Quid pro Quo*, online socijalni inženjering, *pharming,* diverzijska krađa, *Pop-Up* prozori, socijalni inženjering putem telefona, *SMishing, tailgating,* rovarenje po kontejneru, *Robocalls*, krađa važnih dokumenata i *whitelisting flow.*

Zbog promjenljivosti i stalne evolucije prijetnji socijalnog inženjerstva, stvaranje alata za njihovo sprečavanje bi trebalo da bude kontinuiran proces. Ne postoji "savršen" sistem zaštite od ovih prijetnji, ali važno je obučiti ljudski faktor kako bi se suprotstavio ovim napadima (Gulati, 2003).

Postoje i tehnički i netehnički alati i tehnike koje se mogu koristiti za smanjenje rizika povezanih sa socijalnim inženjeringom na nivo kojim se može upravljati i spriječiti da napadi budu uspješni (Odeh *et al*., 2021). Pri tome, smatra se da je prva linija odbrane od napada socijalnim inženjeringom dobro obavljena sigurnosna obuka zaposlenih (Abawajy, 2014).

Kako bi se spriječili upadi u informacione sisteme upotrebom socijalnog inženjeringa, potrebno je implementirati sigurnosne politike i sprovesti trening za edukaciju zaposlenika o neophodnim sigurnosnim procedurama za zaštitu informacija (eng. *SETA – Security Education Training Awareness*) (Patel, 2021).

Dakle, informacioni sistemi podložni su sigurnosnim rizicima, a jedan od najznačajnijih je neadekvatno ponašanje korisnika. S obzirom da je tehnologija nezaobilazan dio svakodnevnog poslovanja, potreba za jačanjem informacione sigurnosti u organizacijama u pogledu zaštite od svih vrsta informacionih prijetnji sve je izraženija (Patel, 2021).

1.2. Ciljevi istraživanja

1. Izložiti osnovne teorijske postulate u vezi sa socijalnim inženjeringom kao prijetnji za sigurnost informacionih sistema (definicija pojma)
2. Objasniti koje vrste napada socijalnim inženjeringom postoje
3. Objasniti faze napada socijalnim inženjeringom
4. Objasniti načine odbrane od napada socijalnim inženjeringom

5. Analizirati percepciju i zaštitno ponašanje korisnika informacionih tehnologija u Bosni i Hercegovini prema prijetnjama od napada socijalnim inženjeringom na informacionu sigurnost

1.3. Istraživačka pitanja

Istraživačko pitanje u ovom master radu raščlanjeno je na više dijelova, te podrazumijeva traženje odgovora na sljedeća pitanja:

1. Postoji li pozitivna korelacija između percepcije korisnika o ozbiljnosti potencijalnih gubitaka usljed napada socijalnim inženjeringom i njihovog straha od ovakvih napada?
2. Postoji li pozitivna korelacija između percepcije korisnika o sopstvenoj ranjivosti i njihovog njihovog straha od ovakvih napada?
3. Postoji li pozitivna korelacija između straha korisnika od napada socijalnim inženjeringom i njihove motivacije za zaštitu od napada?
4. Postoji li pozitivna korelacija između percepcije korisnika o ozbiljnosti potencijalnih gubitaka usljed napada socijalnim inženjeringom i njihove motivacije za zaštitu od ovakvih napada?
5. Postoji li pozitivna korelacija između percepcije korisnika o sopstvenoj ranjivosti i njihove motivacije za zaštitu od napada socijalnim inženjeringom?
6. Postoji li pozitivna korelacija između motivacije korisnika za zaštitu od napada socijalnim inženjeringom i njihovog zaštitnog ponašanja?
7. Postoji li pozitivna korelacija između sprovođenja obuke zaposlenih o sigurnosnim procedurama i njihovog zaštitnog ponašanja?

U skraćenom obliku, istraživačko pitanje možemo svesti na sljedeća dva:

1. Postoji li pozitivna korelacija između motivacije za zaštitu od napada socijalnim inženjeringom (i faktora koji utiču na motivaciju za zaštitu) i zaštitnog ponašanja korisnika?
2. Postoji li pozitivna korelacija između sprovođenja obuke zaposlenih o sigurnosnim procedurama i njihovog zaštitnog ponašanja?

1.4. Hipoteze u istraživanju

U radu će biti testirano sedam hipoteza, prema već postojećim hipotezama autora Patel (2021):

H1: Percipirana **ozbiljnost** potencijalnih gubitaka usljed napada socijalnim inženjeringom je pozitivno korelisana **sa strahom** korisnika od napada socijalnim inženjeringom.

Navedena hipoteza (kao i naredne hipoteze) zasniva se na Teoriji motivacije za zaštitu (eng. *Protection Motivation Theory*, PMT) koja pojašnjava šta motiviše ljude da štite informacije i sisteme u organizacijama u kojima rade. Prvi put opisao je 1975. godine Rogers (1975).

PMT pruža temeljno znanje o tome zašto ljudi možda ne koriste preporučena odbrambena ponašanja kao odgovor na rizike u oblasti informacione sigurnosti (Herath i Rao, 2009). Dakle, Rogers (1975) ističe da ako pojedinac ima više toga za izgubiti (trpiće ozbiljnije posljedice usljed nekog događaja), onda ga je više strah od tog događaja.

Boss *et al.* (2015) takođe u svom istraživanju pokazuju da što je veća ozbiljnost prijetnje za informacionu sigurnost korisnika, to je veća vjerovatnoća da će korisnik imati strah.

H2: Percipirana **ranjivost** korisnika je pozitivno korelisana **sa strahom** korisnika od napada socijalnim inženjeringom.

Što se korisnik smatra lično ranjivijim na napad na informacionu sigurnost, to ga je više strah od napada (Boss *et al*., 2015), što potvrđuje i Patel (2021). Rogers (1975) takođe navodi da ranjivost pojedinca, kada je izraženija, jača strah pojedinca od datog događaja.

H3: Strah korisnika od napada socijalnim inženjeringom je pozitivno korelisan **sa motivacijom** korisnika za zaštitu od napada.

U PMT teoriji, strah (osjećaj koji se javlja kao reakcija na opasnost) je jedan od centralnih konstrukata koji se posebno istražuje, a pri čemu se ističe da veći strah od prijetnje informacionoj sigurnosti rezultira većom motivacijom za zaštitu, što posljedično rezultira sprovođenjem zaštitnog ponašanja pojedinca (Patel, 2021). Takođe, Boss *et al*., (2015) u svom istraživanju pokazuju da kada korisnik ima strah, on će biti više motivisan da se zaštiti.

H4: Percipirana **ozbiljnost** potencijalnih gubitaka usljed napada socijalnim inženjeringom je pozitivno korelisana **sa motivacijom** korisnika za zaštitu od napada.

Procjena prijetnje za informacionu sigurnost korisnika rezultiraće većom motivacijom za zaštitu ako pojedinac smatra da je ozbiljnost posljedica visoka (Sommestad *et al*., 2015). Odnosno, ako korisnik ne smatra da su potencijalni gubici ozbiljni, neće biti motivisan za zaštitu (Sommestad *et al*., 2015).

Boss *et al.* (2015) ističu da ozbiljnost prijetnje direktno utiče na motivaciju za zaštitu, ali i indirektno (posredstvom straha).

H5: Percipirana **ranjivost** korisnika je pozitivno korelisana **sa motivacijom** korisnika za zaštitu od napada.

Procjena prijetnje za informacionu sigurnost korisnika rezultiraće većom motivacijom za zaštitu ako pojedinac smatra da je ranjiviji na tu prijetnju (Sommestad *et al*., 2015). Odnosno, ako korisnik ne smatra da je ranjiv, neće biti motivisan za zaštitu (Sommestad *et al*., 2015).

Takođe, Boss *et al*. (2015) ističu da percipirana ranjivost korisnika direktno utiče na motivaciju za zaštitu, ali i indirektno (posredstvom straha).

H6: Motivacija korisnika za zaštitu od napada je pozitivno korelisana **sa zaštitnim ponašanjem.**

Osnovni model PMT teorije pokazuje da motivacija za zaštitu (eng. *protection motivation*) direktno utiče na zaštitno ponašanje pojedinca (eng. *protection behaviour*) (Sommestad ., 2015). Autori iznose logičan zaključak da kada pojedinac uvidi da postoji velika prijetnja i da se ta opasnost može lako smanjiti kroz određene preventivne mjere, on će osjetiti snažnu motivaciju da se zaštiti primjenom adekvatnog zaštitnog ponašanja. Odnosno, ako je motivacija za zaštitu jaka, pojedinac će djelovati (iskazati zaštitno ponašanje) u skladu sa tom motivacijom (Boss *et al*., 2015).

H7: Sprovođenje **obuke zaposlenih** o sigurnosnim procedurama je pozitivno korelisano **sa zaštitnim ponašanjem**.

PMT u proširenom obliku uvodi i konstrukt obuke zaposlenih (eng. *Security Education Training Awareness, SETA*), a koji ima direktan uticaj na zaštitno ponašanje zaposlenika (Posey *et al*., 2015). Naime, autori u svom istraživanju pokazuju da što je obuka zaposlenika kvalitetnija, to je veća vjerovatnoća da će zaposlenici preduzeti adekvatna zaštitna ponašanja kako bi izbjegli sigurnosne prijetnje.

SETA programi, kako je vidljivo iz naziva, sastoje se od tri osnovna elementa: edukacije, treninga i jačanja svijesti zaposlenika. Ipak, budući da organizacije možda nisu u mogućnosti ili ne žele da se nose sa sva tri navedena zadatka, neke od njih bi mogla prepustiti eksternim saradnicima ili obrazovnim institucijama (Whitman i Mattord, 2022).

Programi obuke pružaju strukturu za planiranje odgovora na prijetnje, edukuju zaposlene o bezbjednosnim problemima sa kojima se njihova kompanija suočava, njihovoj ulozi u odbrani od tih prijetnji i razlozima zbog kojih su te prijetnje usmjerene na njihovu kompaniju (Posey *et al*., 2015).

Svrha *SETA*-e je da poboljša informacionu sigurnost osiguravajući (Whitman i Mattord, 2022):

1. Jačanje svijesti zaposlenih o potrebi zaštite informacionih resursa;
2. Razvoj vještina i znanja kako bi korisnici računara mogli sigurnije obavljati svoje poslove (zaposlenima se pružaju detaljne informacije i praktična uputstva);
3. Stvaranje dubinskog znanja o dizajniranju, implementaciji ili upravljanju sigurnosnim programima za organizacije i sisteme.

Sve navedene aktivnosti doprinose smanjenju rizika od uspješnih napada na informacionu infrastrukturu i osiguravaju da zaposlenici imaju prave alate i znanja za borbu protiv sigurnosnih prijetnji. Neki od primjera su obuka o pravilima i procedurama sigurnog korištenja računara, zaštiti lozinki, prepoznavanju *phishing* poruka, informisanje o novonastalim prijetnjama i slično.

Od navedena tri elementa *SETA* programa, najmanje se koristi jačanje svijesti korisnika, iako je najjeftinije, te može uključivati jednostavne tehnike, kao što su dijeljenje biltena, postera, video zapisa i drugih sitnica koji podsjećaju zaposlene na važnost informacione sigurnosti (Whitman i Mattord, 2022). Autori navode da su od navedenih tehnika, bilteni (eng. *newsletter*) najisplativija metoda širenja sigurnosnih informacija (mogu se distribuirati u papirnom ili digitalnom obliku), te mogu pomoći da se ideja o sigurnosti informacija zadrži u pamćenju korisnika.

Takođe, autori navode da svi zaposleni u organizaciji obavezno moraju biti obučeni i upoznati sa sigurnošću informacija, ali se podrazumijeva da nije svakom članu organizacije potrebna formalna diploma ili certifikat iz oblasti informacione sigurnosti. Takođe, i Grassegger i Nedbal (2021) u svom istraživanju pobijaju hipotezu da *SETA* programi nemaju statistički značajan uticaj na svjesnost pojedinca o informacionoj sigurnosti. Dakle, zanemarivanje sigurnosnih pitanja zbog nedostatka programa podizanja svijesti može značajno povećati rizik od sigurnosnih prijetnji.

1.5. Metodologija istraživanja

Metodologija istraživanja u ovom radu podrazumijeva kombinovanje pregleda već postojeće literature i sprovođenje empirijskog istraživanja.

Pristup empirijskom istraživanju je kvantitativni - sastoji se od prikupljanja podataka, analize podataka, te interpretacije rezultata i donošenja zaključka.

Primarna kvantitativna istraživačka metoda koja će biti korištena u radu je strukturalno modeliranje jednačina (eng. *Structural Equation Modeling*, SEM). SEM metoda se sastoji od dva dijela - prvi dio je konstrukcija matematičkog modela koji opisuje međusobne odnose konstrukata, a drugi dio je korištenje statističkih tehnika za testiranje da li se taj model slaže sa podacima (Civelek, 2018).

SEM metoda u ovom radu podrazumijeva sprovođenje sljedećih koraka:

1. Definisanje konstrukata (percipirana ozbiljnost mogućih gubitaka, percipirana ranjivost korisnika, strah korisnika od napada socijalnim inženjeringom i druge);
2. Konstruisanje hipoteza (npr. hipoteza da postoji pozitivna korelacija između percipirane ozbiljnosti mogućih gubitaka i straha korisnika od napada socijalnim inženjeringom);
3. Prikupljanje podataka (korištenjem odgovarajućeg instrumenata za prikupljanje podataka - ankete);
4. Analiza podataka (koristeći odgovarajući SEM softver podaci će biti analizirani, a hipoteze testirane);
5. Interpretacija rezultata (interpretacija dobijenih rezultata i donošenje zaključaka o relacijama između konstrukata).

Sve postavljene hipoteze biće testirane, a za te potrebe biće korištena već postojeća anketa (Patel, 2021) u skraćenoj verziji, sa ukupno 30 pitanja podijeljenih u šest grupa po pet pitanja. Svaka od tih šest grupa odnosiće se na po jedan konstrukt.

Kroz pitanja u anketi biće istraženo sljedećih šest konstrukata:

1. Percipirana ozbiljnost gubitaka (Patel, 2021, str. 106)
2. Percipirana ranjivost (Patel, 2021, str. 107)
3. Strah (Patel, 2021, str. 108)
4. Motivacija za zaštitu (Patel, 2021, str. 115)
5. Zaštitno ponašanje (Patel, 2021, str. 116)
6. Obuka zaposlenih (eng. *SETA* program) (Patel, 2021, str. 113)

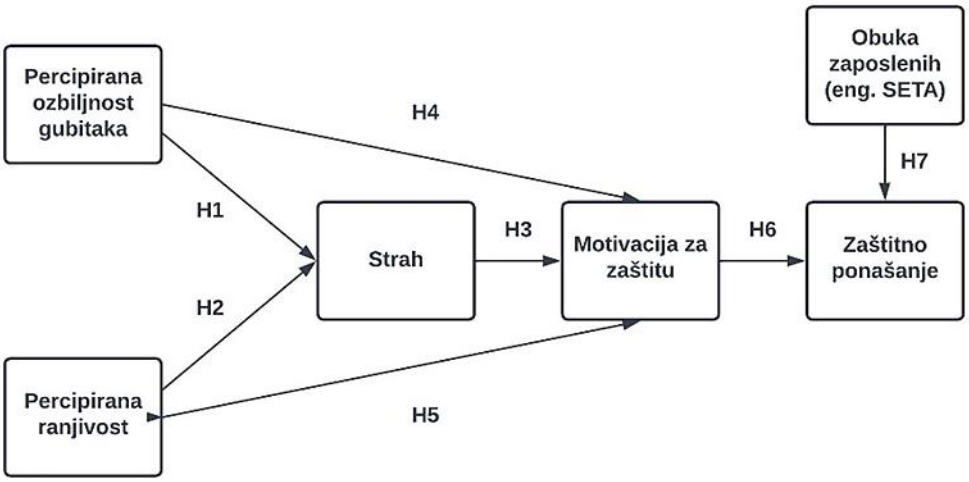
Definicije konstrukata su sljedeće:

1. Percipirana ozbiljnost gubitaka – stav pojedinca o stepenu ozbiljnosti/težine negativnih posljedica koje bi mogle proizaći iz napada socijalnim inženjeringom (Liang i Xue, 2009).
2. Percipirana ranjivost – subjektivni stav pojedinca o vjerovatnoći da će napad socijalnim inženjeringom negativno uticati na njega (Liang i Xue, 2009)
3. Strah – „odgovor na situaciju koja se smatra opasnom i prema kojoj se preduzimaju zaštitne radnje“ (Rogers, 1975, str. 96).
4. Obuka zaposlenih (eng. Security Education Training Awareness, *SETA*) – edukacijski program dizajniran da pomogne organizacijama da umanje broj sigurnosnih propusta uzrokovanih ljudskom greškom (IT Living Lab, n.d.).
5. Motivacija za zaštitu - podstaknutost pojedinca da preduzme korake za zaštitu od napada socijalnim inženjeringom (Boss *et al*., 2015). Motivi za zaštitu mogu biti finansijski, zaštita reputacije i drugi.
6. Zaštitno ponašanje – ponašanje koje služi kao odgovor na prijetnju socijalnog inženjeringa, a koje ima za cilj zaštitu sebe i informacija (Boss *et al*., 2015).

Na primjer, prva hipoteza biće testirana na način da se provede anketa sa korisnicima u kojoj se ispituje njihovo percipirano razumijevanje ozbiljnosti mogućih gubitaka usljed napada socijalnim inženjeringom i njihovog straha od ovakvih napada. Zatim, podaci bi se analizirali koristeći statističku analizu korelacije između navedenih konstrukata. Ako se utvrdi da postoji pozitivna korelacija između ovih konstrukata, to bi podržalo hipotezu da su percipirana ozbiljnost mogućih gubitaka i strah od napada socijalnim inženjeringom pozitivno korelisani. Za svaku narednu hipotezu, postupak je ekvivalentan, s tim što će se ispitivati drugi konstrukti i njihova međusobna veza.

U dijagramu 1. predstavljen je predloženi istraživački model, koji prikazuje međusobne veze svih šest konstrukata, te na koje hipoteze se te veze odnose.

Dijagram 1. Predloženi istraživački model



Izvor: Izrada autora (prilagođeno prema Boss et al., 2015 i Patel, 2021)

Ciljna grupa ispitanika za ovo istraživanje biće zaposleni ljudi koji koriste informacione tehnologije (stariji od 18 godina), a koji žive u Bosni i Hercegovini. Istraživanje će biti sprovedeno korištenjem online alata za sprovođenje anketa. Ispitanici neće biti novčano ili na drugi način kompenzovani za učestvovanje u anketi (davanje odgovora biće dobrovoljno i anonimno).

Ponuđeni odgovori u anketi biće bazirani na Likertovoj skali, kao obliku ordinalne skale pogodne za mjerenje subjektivnih stavova, percepcija i uvjerenja ispitanika. Dobijeni odgovori služiće za testiranje odgovarajućih hipoteza, provjeru korelacije između konstrukata, te za izračunavanje potrebnih statističkih pokazatelja.

Anketa će obuhvatiti i neophodne demografske podatke o ispitanicima koji se odnose na njihov pol, godine, obrazovanje i dosadašnju izloženost napadima socijalnim inženjeringom.

1.6. Struktura završnog rada

Završni rad strukturno je organizovan u četiri poglavlja: uvod, teoretski okvir, metodologija i rezultati empirijskog istraživanja i zaključak. Svako od navedenih poglavlja ponaosob daje doprinos boljem razumijevanju istraživačke teme, ali tek posmatrani kao jedinstvena cjelina stvaraju kompletnu sliku istraživanja.

Uvod (prvo poglavlje) obrazlaže opravdanost predmeta istraživanja socijalnog inženjeringa kao prijetnje sigurnosti informacionih sistema, nudi definiciju ciljeva istraživanja, te postavlja istraživačka pitanja čiji odgovor će pomoći da se postignu postavljeni ciljevi. Takođe, u uvodu su postavljeni temelji teoretskog okvira (drugo poglavlje) jer se poziva na najvažnije naučne radove i teoriju motivacije za zaštitu koja je uslov za definisanje hipoteza. U uvodu je predložen i dijagram istraživačkog modela koji pojašnjava međuodnos konstrukata koji je istražen u trećem poglavlju (metodologija i rezultati empirijskog istraživanja).

Teoretski okvir (drugo poglavlje) strukturiran je u dva zasebna potpoglavlja koja se odnose na ključne pojmove ovog završnog rada. Ovo poglavlje temelji se na sekundarnom istraživanju, odnosno na prethodnim istraživanjima, nudeći pregled relevantne literature. Prvi dio poglavlja posvećen je informacionoj sigurnosti, uključujući definiciju pojma informacione sigurnosti i prijetnji informacionoj sigurnosti. Drugi dio poglavlja posvećen je isključivo socijalnom inženjeringu (uključujući njegovu definiciju, različite vrste napada koji se koriste, faze napada i načine odbrane od ovih napada). Veći akcenat pri pisanju dat je razmatranju socijalnog inženjeringa s obzirom da je upravo on konkretna prijetnja sigurnosti informacionih sistema koja je u fokusu istraživanja.

Metodologija i rezultati empirijskog istraživanja (treće poglavlje) utemeljeni su na primarnom istraživanju. Empirijski pristup istraživanju bio je kvantitativni, a sastojao se od prikupljanja podataka na osnovu sprovedene ankete među stanovnicima Bosne i Hercegovine koji su zaposleni i stariji od 18 godina u vezi sa njihovim stavovima o socijalnom inženjeringu kao prijetnji sigurnosti informacionih sistema. Primarna kvantitativna istraživačka metoda korištena u radu je strukturalno modeliranje jednačina (eng. *Structural Equation Modeling, SEM*), te su obrazložene njene ključne osobine. Detaljno je obrazložen proces prikupljanja podataka, te je dat sveobuhvatan opis uzorka kako bi se dala jasna slika o populaciji koja je predmet istraživanja. Zatim je uslijedila analiza podataka uz primjenu odgovarajućih statističkih metoda, te interpretacija rezultata i donošenja zaključka o prihvatanju ili neprihvatanju postavljenih hipoteza. Za donošenje odluke o statističkoj značajnosti veza među konstruktima korišteni su relevantni statistički pokazatelji, t-statistika i p-vrijednost.

Zaključak (četvrto poglavlje) nudi koncizan pregled i obrazloženje kako su ostvareni ciljevi istraživanja, te potencira doprinos sprovedenog sekundarnog istraživanja, a zatim akcenat stavlja na primarno istraživanje kroz sumiranje rezultata testiranja hipoteza i ograničenja istraživanja.

2. TEORETSKI OKVIR

2.1. Informaciona sigurnost

2.1.1. Definicija pojma informaciona sigurnost

U Merriam-Webster rječniku, sigurnost je definisana kao „stanje oslobođenosti od straha ili opasnosti“. Krećući od ove definicije, definisana je i informaciona sigurnost.

Informaciona sigurnost je stanje, ali i proces očuvanja povjerljvosti, integriteta i dostupnosti digitalnih podataka. Da bi se postigli ovi ciljevi, potrebna je kombinacija alata, tehnologija za upravljanje rizicima, metodologija obuke i drugih specifičnih aktivnosti (Alsharif *et al*., 2022).

Whitman i Mattord (2022) navode da svaka organizacija, bez obzira da li je ona javna ili privatna i bez obzira na njenu veličinu, posjeduje informacije (kao što su podaci o kupcima, proizvodima i uslugama, te zaposlenicima) koje treba zaštiti. Nažalost, nema dovoljno eksperata za informacionu sigurnost, tako da svaki zaposleni mora posjedovati znanje i vještine o tome kako da zaštiti informacije kojima raspolaže, kako bi doprinijeli predupređivanju problema, umjesto da neopreznim postupanjem izazovu probleme u informacionoj sigurnosti (Whitman i Mattord, 2022).

Prema definiciji CNSS-a (eng. National Security Agency's Committee on National Security Systems), informaciona sigurnost predstavlja proces zaštite informacija i informacionih sistema od neovlaštenog pristupa, korišćenja, otkrivanja, uništavanja, ometanja, krađe, gubitka i oštećenja (Whitman i Mattord, 2022). Cilj unapređenja i održavanja informacione sigurnosti je zaštita, pouzdanost, integritet, dostupnost i autentičnost informacija koje organizacija posjeduje (eng. C.I.A Triad – confidentiality, integrity and availability). Ova definicija naglašava važnost zaštite informacija i informacionih sistema od štetnih uticaja (internih i eksternih), a istovremeno ističe potrebu za održavanjem funkcionalnosti i pouzdanosti informacionih sistema.

U većini literature, termini "informaciona sigurnost" i "sajber sigurnost" koriste se kao sinonimi. Međutim, autori Reid i Van Niekerk (2014) u svom istraživačkom radu predlažu da se napravi razlika između ovih termina. Naime, oni smatraju da je sajber sigurnost širi pojam od informacione sigurnosti. Sajber sigurnost obuhvata ne samo zaštitu informacija, već i drugih sredstava, uključujući i ljude. U odnosu na informacionu sigurnost, ljudski faktor u sajber sigurnosti se odnosi ne samo na ulogu ljudi u zaštiti informacija, već i na njihovu ulogu kao potencijalnih meta sajber napada ili čak nesvjesnih učesnika u takvim napadima. Ipak, zbog jednostavnosti, u ovom master radu oba termina (informaciona i sajber sigurnost) biće korišteni kao sinonimi – odnosno u oba termina u razmatranje će biti uključen i ljudski faktor.

Jedan od ključnih koncepata u informacionoj sigurnosti je i kriptografija. Osnovnu terminologiju kriptografije prema Stamp (2011) čine kriptologija (nauka i umjetnost stvaranja i otkrivanja „tajnih kodova“), kriptografija (stvaranje „tajnih kodova“) i kriptoanaliza (otkrivanje „tajnih kodova“). Razlog zašto treba spomenuti kriptografiju u kontekstu teme ovog master rada je u tome što se socijalni inženjering često koristi kao tehnika kojom se napadači pokušavaju domoći tajnih ključeva i drugih podataka koji se koriste za kriptografske svrhe. Na primjer, napadači mogu pokušati da preuzmu kontrolu nad računarem žrtve pomoću nekog malicioznog programa, kako bi otkrili tajni ključ ili lozinku koja se koristi za enkripciju podataka. Takođe, napadači mogu pokušati da preuzmu kontrolu nad serverima koji se koriste za enkripciju i dekripciju podataka. Međutim, socijalni inženjering koristi ljudsku slabost i manipulaciju kako bi dobili informacije koje su potrebne za pristup zaštićenim podacima. Dakle, kriptografijom se načelno ne može zaštiti od napada socijalnim inženjeringom, ali se napadačima može otežati i usporiti proces iskorištavanja podataka do kojih su došli ako su oni enkriptovani, umjesto napisani običnim tekstom.

Kriptografija ima važnu ulogu u zaštiti od napada na sigurnost informacionih sistema, ali za potpunu zaštitu od napada socijalnim inženjeringom, potrebno je koristiti i druge metode i pristupe. Kombinacijom različitih pristupa stvara se jača linija odbrane od napada socijalnim inženjeringom i svih drugih prijetnji informacionoj sigurnosti.

2.1.2. Prijetnje informacionoj sigurnosti

Napadi na informacione sisteme neminovan su pratilac razvoja informacionih tehnologija. Vrijednost koju informacije imaju može donijeti finansijske ili druge koristi napadačima, zbog čega oni pribjegavaju korištenju različitih, pa čak i neetičkih, metoda da dođu do željenih informacija. Štete koje proizilaze iz realizacije prijetnji koje ugrožavaju informacioni sistem variraju u razmjerama i ozbiljnosti, ali po pravilu dovode do negativnih posljedica. Šteta može biti neznatno mala, ali i ozbiljnija, pa čak i dovesti do potpunog uništenja cjelokupnog sadržaja i funkcionalnosti informacionog sistema.

Prijetnje se mogu pojaviti usljed različitih događaja, na primjer usljed nemarnog ponašanja zaposlenika ili hakerskih napada (Jouini *et al*., 2014).

Prijetnje sigurnosti informacionih sistema eksploatišu ranjivosti sistema koje postoje, što povećava sigurnosne rizike. Pri tome, ranjivosti predstavljaju slabosti informacionog sistema koje napadači mogu iskoristiti da zaobiđu zaštitne mehanizme i otvore sebi put prema povjerljivim informacijama organizacije (Jouini *et al*., 2014).

Osnovna podjelom prijetnji je podjela s obzirom na to da li prijetnje dolaze iz internih izvora (zaposlenici, poslovni partneri i sl.) ili eksternih (npr. hakeri). Ipak, postoji više različitih načina na koje se može izvršiti klasifikacija prijetnji informacionoj sigurnosti. Autori Jouini *et al*. (2014), ističu da se sve vrste klasifikacija prijetnji mogu se podijeliti u dvije velike i sveobuhvatne grupe:

1. Klasifikacije prijetnji informacionoj sigurnosti s obzirom na tehniku izvođenja napada (npr. korištenjem zlonamjernog softvera, mrežnim napadom, fizičkim napadom i sl.)
2. Klasifikacije prijetnji informacionoj sigurnosti s obzirom na posljedice napada (najpoznatiji je STRIDE model koji koristi Microsoft, a koji prijetnje klasifikuje s obzirom na motive napadača)

Bez obzira na način na koje se vrše klasifikacije prijetnji, u okviru svih je nezaobilazna i prijetnja informacionoj sigurnosti u vidu napada socijalnim inženjeringom (Duarte *et al*., 2021).

Prema nalazima Wulandari *et al*. (2022) studije, na podložnost napadu socijalnim inženjeringom ne utiče nijedan demografski faktor. Odnosno, autori ističu da starost, pol, nivo obrazovanja, zanimanje i socioekonomski status neke osobe ne moraju biti pokazatelj da li je osoba manje ili više osjetljiva na napad socijalnim inženjeringom – svi mogu biti žrtva. Međutim, studija Albladi *et al*. (2020) ima drugačije rezultate po ovom pitanju.

Tačnije, njihovi rezultati pokazuju da pol ima uticaj na ranjivost žrtve (žene su podložnije napadima), vrsta stečenog obrazovanja ima uticaj na ranjivost žrtve (pojedinci koje imaju obrazovanje iz oblasti tehničkih nauka manje su ranjivi na napade socijalnim inženjeringom), te da godine nemaju statistički značajan uticaj na ranjivost korisnika. Ipak, kada su autori uporedili prosjeke godina ispitanika, uočili su da su mlađe osobe manje podložne napadima nego starije. Zajednički zaključak obje navedene studije je da nivo formalnog obrazovanja nema statistički značajan uticaj na ranjivost korisnika.

Studija Wulandri *et al*. (2022) studija pokazuje da to što neko ima više ili manje IT vještina nije presudan faktor, ni dobar prediktor sklonosti osobe da postane žrtva napada. Umjesto toga, istraživanje identifikuje tri glavna faktora koji utiču na ranjivost na ovakve napade:

1. Navika - često ažuriranje statusa na društvenim mrežama (autori koriste primjer WhatsApp-a) ili povećavanje broja konekcija povezano je sa većom podložnošću napadu;
2. Osjećaj rizika - dobro razumijevanje opasnosti od napada i mogućnosti da on rezultira štetom može smanjiti šansu da neko postane žrtva;
3. Iskustvo - što se učestalost i varijabilnost napada povećava, to je veći rizik da će neko najzad i postati žrtva.

2.2. Socijalni inženjering

2.2.1. Definicija pojma socijalni inženjering

Prije nego definišemo socijalni inženjering akademskim rječnikom, možemo zamisliti jedan slikovit primjer socijalnog inženjeringa iz svakodnevnog života. Na primjer, svom prijatelju želite napraviti tortu za rođendan, ali ne znate kako biste je dekorisali i koje boje biste upotrijebili. Budući da torta treba da bude iznenađenje, ne želite pitati direktno koju boju voli. Tada koristite socijalni inženjering – suptilniji pristup, pri kome spominjete da je u trendu neka boja odjeće, pa pitate prijatelja šta o njoj misli. Vaš prijatelj, nesvjesno, počinje razmišljati o svojim preferencijama i spominje svoju omiljenu boju. U ovom scenariju, vi ste koristili svoje "društvene vještine" kako biste postigli svoj cilj - saznali omiljenu boju vašeg prijatelja. Analogno tome, socijalni inženjering u kontekstu informacionih tehnologija podrazumijeva korištenje manipulativnih taktika kako bi se izvukla informacija ili ostvario pristup osjetljivim podacima. Umjesto da se koriste tehničke ranjivosti, kao u slučaju hakerskog napada, socijalni inženjering iskorištava ljudsku prirodu i sklonost da dijelimo informacije ili obavljamo tražene radnje bez puno razmišljanja.

Upravo napadi socijalnim inženjeringom i jesu jedna od glavnih prijetnji i najrasprostranjenijih i najuspješnijih vrsta napada na sigurnost informacionih sistema (Duarte *et al*., 2021). Razlog je u tome što iskorištavaju neoprezno ljudsko ponašanje, a ne tehničke ranjivosti, zbog čega ih može biti teško otkriti i spriječiti. Najopasnija osobina socijalnog inženjeringa je upravo u tome što se većinski oslanja na grešku krajnjeg korisnika, a u manjoj mjeri na tehnološke propuste (Patel, 2021). Khonji *et al*. (2013) ističu da se mnogi

sajber napadi šire pomoću mehanizama koji eksploatišu slabosti krajnjih korisnika, što znači da su krajnji korisnici najslabija karika lanca sigurnosti. Krombholz *et al*. (2015) smatraju i da je socijalni inženjering superiorniji od većine drugih oblika hakovanja zbog toga što može probiti zaštitne mehanizme čak i najsigurnijih informacionih sistema, a zahvaljujući mogućnosti automatizacije u nekim slučajevima, može se primijeniti i na široj populaciji.

Na socijalni inženjering kao prijetnju sigurnosti informacionih sistem još uvijek nije dovoljno pažnje obraćeno u pogledu formalnih definicija, okvira i obrazaca izvođenja napada (Mouton *et al*., 2016).

Socijalni inženjering je postupak manipulisanja korisnikom kako bi on obezbijedio određene informacije ili preduzeo određene aktivnosti kojima se ugrožava informaciona sigurnost (Patel, 2021). Odnosno, socijalni inženjering je tehnika kojom se manipuliše ljudima tako da oni svjesno ili nesvjesno omoguće pristup informacionom sistemu napadaču koji nije autorizovan da mu pristupi (Hadnagy, 2010).

Napadači manipulišu žrtve kako bi dobili povjerljive informacije koje se mogu koristiti za postizanje različitih ciljeva ili prodati na crnom tržištu i *dark web*-u (Salahdine i Kaabouch, 2019).

Meta napada mogu biti pojedinci, grupe pojedinaca ili organizacije (Mouton *et al*., 2016). Organizacije koju su često pod napadima su finansijske institucije, obrazovne i zdravstvene institucije i slično (Yasin *et al*., 2019). Međutim, nijedna organizacija nije imuna na napade, pa stoga svaka organizacija treba da ima plan za zaštitu od napada.

Prijetnja koju predstavlja socijalni inženjering je univerzalna zbog neizbježnog postajanja ljudskih slabosti u pogledu njihovog odnosa prema informacionoj sigurnosti (Wang *et al*., 2020). Socijalni inženjering je netehnička metoda iskorištavanja znanja o ljudskoj psihologiji i ponašanju kako bi se dobio pristup povjerljivim informacijama ili sistemima. Bez obzira na to koliko dobro su razvijene i implementirane mjere sigurnosti, ne postoji računarski sistem na svijetu koji u krajnjoj liniji ne zavisi od ponašanja ljudi. Ljudi kao faktor informacione sigurnosti ne samo da su podložni potpadanju pod uticaj socijalnog inženjeringa, već često predstavljaju najznačajniju slabu tačku, odnosno ranjivost informacionih sistema u poređenju sa svim ostalim ranjivostima informacionih sistema (Wang *et al*., 2020).

Samo jedna ljudska greška je dovoljna da neko postane žrtva napada socijalnim inženjeringom. Napadači često primjenjuju tehniku socijalnog inženjeringa jer je jednostavnije koristiti ljude kao objekat zloupotrebe, nego izdvojiti vrijeme i steći naprednije vještine potrebne za pronalaženje ranjivosti tehničke prirode u informacionim sistemima (Jones, 2022). Napadači suptilno manipulišu ljudskim emocijama, izazivajući osjećaj straha, uzbuđenosti ili hitnosti. Upravo iz ovih razloga, napadači sve češće koriste koriste strategije socijalnog inženjeringa.

Ljudi često bivaju naivni – previše povjerljivi ili žele pomoći, usljed čega (čak i kada su zaštićeni jakim sigurnosnim mjerama) postaju meta napadača koji manipulacijom dolaze do povjerljivih informacija (Wang *et al*., 2020).

Ljudske radnje koje bi mogle ugroziti organizaciju uključuju slučajno ili namjerno otkrivanje kredencijala trećim stranama, nasjedanje na *phishing* e-poruke klikom na ugrađene veze na web stranicama i instaliranje nepoznatih medija ili softvera na lične ili radne računare (Parsons *et al*., 2014).

Žrtva mora imati asimetričan odnos znanja sa napadačem kako bi socijalni inženjering funkcionisao. Napadač zatim koristi ovu asimetriju kako bi nametnuo tehnokratsku kontrolu nad žrtvom (Hatfield, 2018). Međutim, ukoliko žrtva ima visok nivo svijesti o opasnostima socijalnog inženjeringa, mogućnost da bude prevarena se smanjuje. Zbog toga je izuzetno važno da kompanije redovno obučavaju svoje zaposlene i pružaju im informacije o najnovijim metodama napada.

Praksa socijalnog inženjeringa kao metode manipulisanja ljudima kako bi se došlo do željenih informacija postoji otkad i samo čovječanstvo (Mitnick Security Consulting, n.d.). Po riječima Kevina Mitnicka (2002), mnogo je lakše nekoga prevariti da Vam otkrije svoju lozinku nego trošiti vrijeme i resurse da zaista tehnički prodrete u informacioni sistem. Termin „socijalni inženjering“ prvi je upotrijebio britanski ekonomista Džon Grej u svojoj knjizi „Efikasan lijek za nevolje nacija“ o zamjeni zlatnog standarda za razmjenu valutom, objavljenoj 1842. godine (Hatfield, 2018).

Prelaz socijalnog inženjeringa iz sfere fizičkog svijeta u digitalni neminovan je rezultat potrebe za digitalnim informacijama sadržanim u informacionim sistemima, a koje imaju inherentnu vrijednost za onog ko ih posjeduje.

Stoica (2021) ističe da su prikupljanje informacija putem telefonskog poziva i lažno predstavljanje u elektronskim porukama česta taktika u socijalnom inženjeringu. Poruke i pitanja napadača se nastoje predstaviti tako da izgledaju kao da potiču iz legitimnih izvora, koristeći logo kompanija ili često posjećivane web stranice kako bi obmanule žrtve da povjeruju u sadržaj poruke i da preduzmu tražene radnje. Danas je potrebno samo nekoliko sekundi da se pronađe logo kompanije, njena upravljačka struktura i organizacijski dijagram, što olakšava njihovo korištenje za prenošenje malicioznih poruka koje izgledaju vjerodostojno. Što je imitacija uvjerljivija, veća je vjerovatnoća uspjeha u obmanjivanju žrtve, čak i kod iskusnih korisnika, koji bi inače bili u stanju da uoče lažno predstavljanje (Stoica, 2021).

Prema istraživanju Verizona (2022), napadi socijalnim inženjeringom bili su najčešći tip sigurnosnih incidenta u njihovom Izvještaju o istragama kršenja podataka za 2022. godinu. Takođe, navode i da je čak 82% curenja podataka povezano sa ljudskim faktorom, a pri tome najčešće se javljaju *phishing* i *pretexting* napadi.

2.2.2. Vrste napada socijalnim inženjeringom

Salahdine i Kaabouch (2019) sumiraju da postoji dvadeset različitih vrsta napada socijalnim inženjeringom: *phishing*, korištenje mamca (eng. *baiting*), *pretexting, ransomware,* gledanje preko ramena, obrnuti socijalni inženjering, korištenje lažnog softvera, lažno predstavljanje na pozivima službi za pomoć, *Quid pro Quo*, online socijalni inženjering, pharming, diverzijska krađa, Pop-Up prozori, socijalni inženjering putem telefona, *SMishing, tailgating,* rovarenje po kontejneru, *Robocalls*, krađa važnih dokumenata i *whitelisting flow*.

2.2.2.1. Phishing

Izraz *phishing* osmišljen je kao asocijacija na englesku riječ *fishing* (pecanje), povlačeći paralelu da ribari (tj. napadači) koriste mamac (tj. socijalnim inženjeringom osmišljene poruke) za pecanje (npr. krađu ličnih podataka žrtava) ističe Khonji *et al*. (2013).

Phishing je jedna od najčešće korišćenih i najefikasnijih tehnika socijalnog inženjeringa koje sajber kriminalci koriste za pristup važnim i osjetljivim informacijama. Studija Radne grupe za borbu protiv *phishing*-a (Anti-Phishing Working Group, 2022) pokazuje da je u trećem kvartalu 2022. godine bilo ukupno 1.270.883 *phishing* napada na globalnom nivou, što je najveći broj *phishing* napada u jednom kvartalu od kad APWG prati *phishing* napade (od 2008. godine).

APWG (2022) definiše *phishing* kao kriminalnu aktivnost koja kombinuje taktike socijalnog inženjeringa i tehničke prevare za krađu ličnih podataka i kredencijala finansijskih računa korisnika. Dakle, u pitanju je taktika u kojoj napadač šalje e-mail poruku preko koje od primaoca pokušava izvući povjerljive informacije. Uspješnost ovih napada zasnovana je na neopreznosti žrtava, koje su obmanute tako da misle da komuniciraju sa legitimnim partnerom, jer šalje e-poštu za koju se čini da dolazi iz legitimnog izvora, odnosno koristi e-mail adrese koje izgledaju pouzdano. Lažne web stranice su dizajnirane da privuku žrtvu i da ih navedu na unos informacija kao što su korisničko ime i lozinka. Takođe, ukoliko korisnik nije oprezan, malware može biti instaliran i na njegov računar i služiti za direktnu krađu kredencijala. Na primjer, Heartfield i Loukas (2015) izdvajaju primjer da USB uređaj za pohranu podataka može biti unaprijed zaražen Microsoft Word datotekom koja izgleda legitimno, ali zapravo sadrži zlonamjerni Visual Basic makro ili kod za izvođenje napada nultog dana (eng. zero-day attack). Kada korisnik klikne na datoteku, Microsoft Word se otvara kao i obično, ali istovremeno pokreće zlonamjerni kod koji je povezan s Word dokumentom, navode autori.

Stoga, važno je da korisnici budu svjesni opasnosti i da razumiju taktike *phishing* napada. U slučaju primanja sumnjivih e-mail poruka ili neuobičajenih aktivnosti na računaru, bolje je sačekati i izvršiti sigurnosne provjere, nego bespogovorno slijediti linkove ili upute date u bilo kojoj e-mail poruci.

Da bi se sistemi zaštitili od *phishing* napada, mora se koristiti kombinacija obuke za podizanje svijesti zaposlenih o sajber napadima, sigurni nalozi za e-poštu, filtriranje URL-ova, te brza identifikacija *phishing* lokacija (Alabdan, 2020).

Phishing se najčešće vrši preko e-mail poruka, ali postoje i druge vrste *phishing*-a, kao što su *SMishing i vishing* (Yeboah-Boateng i Amanor, 2014). Za razliku od uobičajenog načina sprovođenja napada (e-mail *phishing*), kod SMishing napada napadač šalje poruke putem SMS-a sa lažnim poveznicama ili ponudama. S druge strane, *vishing*, odnosno *voice phishing*, podrazumijeva glasovne pozive žrtvi tokom kojih se prikupljaju povjerljive informacije. U sva tri slučaja, napadači se lažno predstaviljaju kao pouzdane osobe ili organizacije. Zajedničku svrha svih vrsta *phishing*-a je obmanjivanje žrtve da da svoje podatke, bilo putem elektronske pošte, tekstualnih poruka ili glasovnog poziva. Cilj svih vrsta *phishing*-a je da se žrtvino povjerenje zloupotrijebi kako bi se dobile važne informacije.

2.2.2.2. Baiting

Korištenje mamca (eng. *baiting*) je slično *phishing*-u, ali je specifično po tome što se žrtva nagovara da izvrši određenu radnju u zamjenu za neku nagradu. Na primjer, napadač može obećati besplatne stvari, kao što su telefoni, novčane nagrade i slično, ako se žrtva prijavi sa svojim podacima na neku (malicioznu) stranicu ili podijeli neke lične informacije (Lohani, 2019). Takođe, napadači nekad dijele zaražene USB-ove kao „poklone“ koji sadrže zlonamjerni softver koji se može koristiti za napad na mrežu kompanije (Lohani, 2019). *Baiting* se često izvodi putem e-mail poruka i reklama, a često se može vidjeti i na neprovjerenim web stranicama i *dark web*-u.

Primjer *baiting*-a je i klasični scenario u kome napadač ostavlja zaraženi USB na prometnom mjestu, s nadom da će ga neko uzeti i priključiti na svoj računar. Mamac (eng. bait) je postavljen s namjerom da izazove znatiželju i želju prolaznika da ga pokupi i pokuša saznati šta se nalazi na USB-u ili kome pripada. Nakon što korisnik poveže USB s vlastitim računarem, aktivira se zlonamjerni sadržaj pohranjen na tom uređaju, a koji izlaže informacioni sistem riziku od krađe podataka, neovlaštenog pristupa, a čak može otvoriti i mogućnost za uspostavljanje kontrole računara na daljinu.

2.2.2.3. Pretexting

Pretexting napadi se baziraju na stvaranju lažne, ali uvjerljive priče kako bi se prikupili podaci žrtve (Salahdine i Kaabouch, 2019). Odnosno, to je taktika pri kojoj napadač stvara lažni identitet ili scenario kako bi prevario pojedince da daju osjetljive informacije.

Riječ *pretext* u ovom slučaju podrazumijeva lažni izgovor za kontaktiranje žrtve (npr. napadač traži hitan odgovor na postavljena pitanja jer mu je dijete bolesno) kojim se prikriva stvarni razlog kontaktiranja žrtve (dobijanje informacija potrebnih za krađu informacija).

Ova lažna priča djelovaće na emocije žrtve, izazivajući sažaljenje, usljed čega ona dijeli tražene informacije.

Autori Salahdine i Kaabouch (2019) navode da se *pretexting* napad može izvesti putem telefonskog poziva, e-pošte ili ličnog kontakta sa žrtvom. Da bi izveli svoj plan, napadači često skupljaju informacije koje su javno dostupne putem telefonskih imenika ili javnih web stranica, a zatim ih koriste za stvaranje lažnog privida o svom znanju, identitetu i namjerama. Napadač može koristiti izgovore za kontaktiranje žrtve poput traženja posla, nuđenja usluga, traženja pomoći za prijatelja koji je izgubio pristup nečemu ili davanje informacija o lažnim nagradnim igrama (Salahdine i Kaabouch, 2019). Napadači najčešće telefoniraju ili ostavljaju govornu poštu pretvarajući se da su iz legitimne organizacije, poput banke ili vladine agencije, kako bi naveli pojedince da daju osjetljive informacije ili im prenesu novac.

Čest je primjer i da se napadač predstavlja kao neko iz IT sektora kompanije u kojoj je žrtva zaposlena (Mitnick, 2002). Napadač obavještava žrtvu da je primijetio neke "probleme" sa računom žrtve, te tvrdi da su mu zbog toga potrebni određeni podaci kako bi navodno riješio dati problem. Na taj način, ukoliko je žrtva lako povjerljiva i nema ranijeg iskustva sa ovakvim vrstama prevara, brzo se dolazi do potrebnih podataka koji će kasnije biti iskorišteni. U ovom primjeru može se uočiti da napadač koristi prethodno istraživanje prilikom koga se upoznaje se strukturom kompanije kako bi bio uvjerljiv i povećao vjerovatnoću uspješnog izvođenja prevare.

S druge strane, umjesto da se predstavljaju kao predstavnik ili zaposlenik neke kompanije, u *pretexting* napadima napadač može i da se lažno predstavlja kao klijent kompanije, takođe putem telefonskog poziva. Ovakvi napadi često su usmjereni upravo protiv kompanija koje skladište podatke o svojim klijentima, kao što su bankarske institucije, pružaoci komunalnih usluga i saobraćajna preduzeća (Wilhelm, 2013). U ovom slučaju, *pretexting*-om se iskorištava nedostatak u metodama identifikacije klijenata koje kompanije primjenjuju prilikom telefonskog razgovora sa klijentom (Wilhelm, 2013). Budući da fizička identifikacija nije moguća, poslovni subjekti moraju identifikovati svoje korisnike na druge načine (traženjem potvrde ličnih podataka kao što su adresa stanovanja, datum rođenja, djevojačko prezime majke ili broj računa). Međutim, do većine ovih podataka često se može doći jednostavnim pretraživanjem društvenih mreža ili kopanjem po smeću žrtve, što predstavlja jasnu ranjivost kompanija i pojedinaca i povećava mogućnost zloupotrebe. Informacije koje su lako dostupne putem interneta ili koje se bacaju u smeće bez odgovarajuće zaštite mogu biti iskorištene za izvođenje različitih zlonamjernih aktivnosti.

2.2.2.4. Scareware

Scareware je vrsta zlonamjernog softvera koji se širi korištenjem straha i lažnih upozorenja o virusima, sigurnosnim propustima i sličnim prijetnjama računaru ili podacima korisnika (Siddiqi *et al*., 2022). Cilj je da žrtva klikne na poruku ili link i instalira maliciozni program,

koji zatim zahtijeva plaćanje za uklanjanje štete ili za smanjenje rizika od budućih napada. Ova vrsta zlonamjernog softvera često se širi putem e-pošte ili kroz reklame na nezvaničnim ili sumnjivim web stranicama. *Scareware* softver koristi boje, fontove i logotipe koji su slični poznatim brendovima antivirusnog softvera ili drugih proizvoda, kako bi zavarali žrtvu (Malin *et al*., 2017).

Scareware možemo podijeliti u sljedeće dvije grupe:

1. Lažno antivirusno upozorenje koje korisnik prima na e-mail s naslovom "Vaš računar je ozbiljno zaražen!" ili sličnim. Poruka tvrdi da je korisnikov računar u opasnosti i treba hitno reagovati kako bi se spriječila daljnja šteta (Siddiqi *et al*., 2022). U poruci se nalazi link koji navodno vodi do besplatnog antivirusnog skenera za uklanjanje virusa. Kada korisnik klikne na link, preusmjeren je na web stranicu koja izgleda slično stranici poznatog antivirusnog softvera, ali zapravo instalira maliciozni softver na računar korisnika.
2. Nasumično iskačuće upozorenje (eng. pop-up) na web stranici koju korisnik posjećuje, a koje prikazuje riječi "Vaš računar je ugrožen virusima!" ili slično upozorenje (Thomas *et al*., 2020). Upozorenje sadrži animaciju koja simulira skeniranje računara i otkriva lažne prijetnje. Nudi opciju "ukloni viruse odmah" koja vodi do stranice gdje korisnik može "preuzeti besplatan alat za čišćenje", kao i u prethodnom primjeru. Klikom na ovu opciju, korisnik zapravo preuzima i instalira zlonamjerni softver koji kasnije zahtijeva plaćanje za "čišćenje".

Korištenje straha kao glavnog pokretača za podsticanje korisnika da donesu brze i nepromišljene odluke posredstvom obmanjujućih upozorenja i privlačnih opcija za "rješavanje problema“ pokazalo se kao vrlo uspješna tehnika socijalnog inženjeringa. *Scareware* zloupotrebljava prirodni instinkt korisnika da se brine za svoju sigurnost i preduzme nešto kako bi se osjećao kao da je učinio sve u svojoj moći da spriječi veću štetu.

Napadači mogu čak i prilagoditi sadržaj i poruke *scareware*-a prema specifičnim karakteristikama ciljne publike. Na primjer, ako napadaju određenu demografsku grupu ili industriju, *scareware* poruke mogu biti prilagođene njihovim ličnim interesima i navikama. Razlog primjenjivanja postupka prilagođavanja *scareware*-a je u tome što su korisnici više skloni da reaguju na poruke koje se čine relevantnim i prilagođenim njihovim potrebama i iskustvu. Navedena mogućnost prilagođavanja *scareware*-a ciljnoj publici dodatno povećava njegovu opasnost i učinkovitost.

2.2.2.5. Dumpster diving

U potpunosti netehnološka metoda za dolaženje do informacija je i kopanje po smeću (eng. *dumpster diving*). Postupak se sastoji od pretraživanja smeća koje je meta napada bacila, a u cilju pronalaženja papira sa važnim informacijama (npr. lozinkama ili podacima o kreditnoj kartici) (Siddiqi *et al*., 2022).

Pretraživanjem smeća napadači traže i informacije kao što su organizaciona hijerarhija i ko je kome nadređen (uključujući imena, titule i kontakt informacije), posebno na menadžerskom nivou, kako bi se mogli lažno predstavljati kao nadređeni ili podređeni i tako doći do dodatnih željenih informacija (Bansla *et al*., 2019). Odnosno, informacije dobijene sakupljanjem smeća mogu se kasnije koristiti i u *pretexting* napadima. Iako je ovakva vrsta napada česta, sprečavanje je relativno jednostavno – potrebno je samo na odgovarajući način uništiti svu dokumentaciju koja sadrži povjerljive informacije tako da one nikad ne dospiju u ruke neovlaštenih osoba.

2.2.2.6. Obrnuti socijalni inženjering

Obrnuti socijalni inženjering podrazumijeva da se žrtvi pravi privid da je ona sama pristupila napadaču, a ne napadač njoj. Naime, napadač u ovom slučaju potajno kreira neki problem za žrtvu, a zatim se prikazuje kao neko ko može riješiti taj problem i nudi svoju pomoć (Parthy i Rajendran, 2019). Kada stekne povjerenje mete, on se postepeno upušta u razgovore o sve privatnijim i povjerljivijim temama, bilo da se radi o poslovnom ili privatnom životu mete. Obrnuti socijalni inženjering koristi se da bi se uticalo na zaposlene na ključnim pozicijama, jer su oni češće pod stresom i usljed toga lakše je manipulisati njima (Irani *et al*., 2011).

Dakle, ključna karakteristika ovog pristupa je podsticanje žrtava da same iniciraju kontakt s napadačem, efektivno koristeći obrnuti smjer interakcije u odnosu na standardni pristup socijalnim inženjeringom. Koyun i Al Janabi (2017) objašnjavaju obrnuti socijalni inženjering na narednom primjeru. Na primjer, ako napadač direktno pozove korisnika telefonom, predstavi se kao sistem administrator i pita ga za njegovu lozinku, korisnik će vjerovatno biti sumnjičav i neće je otkriti. Međutim, upotrebom obrnutog socijalnog inženjeringa mogao bi se preduprijediti taj problem. Naime, nekoliko dana ili sedmica ranije, korisnicima se može poslati e-mail od (lažnog) sistem administratora u kojem se navodi da u slučaju problema korisnici mogu pozvati u e-mail-u navedeni telefonski broj za podršku. Zahvaljujući korištenju ove strategije, idući put kada korisnici budu u neprilici, oni će samoinicijativno pozvati naznačeni broj tražeći pomoć, te bez problema otkriti svoju lozinku lažnom administratoru sistema. Cijela situacija će se odvijati bez sumnje u kredibilnost lažnog administratora, upravo zbog toga što je korisnik samostalno inicirao kontakt. Na kraju, možemo zaključiti da pristup obrnutog socijalnog inženjeringa ukazuje na to da je duboko razumijevanje ljudskog ponašanja i psihologije ključno za uspješnu manipulaciju i ostvarivanje napadačkih ciljeva.

2.2.2.7. Druge vrste socijalnog inženjeringa

Praćenje (eng. *tailgating*) je tehnika socijalnog inženjeringa koja neovlaštenim osobama omogućava pristup prostorijama kojima mogu pristupiti samo zaposleni. Napadač fizički prati žrtvu koja ima legitiman pristup kroz sigurna vrata, te koristi trenutak nepažnje i užurbanosti žrtve. Kada žrtva ostvari prolaz u određenu prostoriju (npr. pomoću pametne

kartice), napadač je zamoli da pridrži vrata ili bez direktnog kontakta sa žrtvom ulazi kroz otvorena vrata prije nego što se ona zatvore (Breda *et al*., 2017). Korištenjem mjera sigurnosti poput uvođenja pravila da samo jedna osoba smije proći kroz vatra u određenom trenutku moguće je smanjiti rizik od *tailgating*-a.

Gledanje preko ramena (eng. *shoulder surfing*) je tehnika socijalnog inženjeringa u kojoj napadač fizički direktno gleda preko ramena žrtve dok ona radi, pri tome posmatrajući sadržaj ekrana žrtve ili šta ona piše na tastaturi bez njenog znanja ili odobrenja u cilju otkrivanja važnih informacija (Krombholz *et al*., 2015). Takođe, može uključivati ne samo direktno posmatranje ekrana žrtve, već i papirne dokumentacije koja je na stolu i slično. Ova tehnika često se koristi u kombinaciji sa drugim tehnikama socijalnog inženjeringa, kao što su *tailgating* ili *phishing*. Zaposlenici se mogu zaštititi od ove tehnike tako što će okrenuti ekran i tastature od pogleda drugih osoba kako bi smanjili rizik od curenja informacija usljed gledanja preko ramena.

„Vodena rupa“ (eng. *waterholing*) je ciljani napad socijalnim inženjeringom u kome napadači vrše izmjene na web stranici za koju se zna da je posjećuju ciljani pojedinci. Odnosno, ovo strategija se temelji na iskorištavanju povjerenja koje korisnici imaju prema web stranicama koje redovno posjećuju (Abass, 2018). Nakon postavljanja zamke, napadači jednostavno čekaju da žrtva unese svoje kredencijale na lažnoj stranici (koja je imitacija prave stranice), kako bi ih iskoristili za pristup ciljanim mrežama i sistemima (Edwards *et al*., 2017). Napad se obično sprovodi na već kompromitovanim stranicama, tako da napadači zamijene originalne stranice s lažnim formama za prijavu kako bi prikupili korisničke podatke. Naročita opasnost od ovog napada ogleda se u tome što žrtve često ne sumnjaju u autentičnost stranice na kojoj unose svoje podatke. Naime, pojedinci imaju sklonost da sa manje opreza koriste stranice koje su ranije posjećivali. Ovaj fenomen proizilazi iz psihološkog principa poznatog kao "*familiarity bias*", a koji ukazuje da ljudi više vjeruju u ono što im je odranije poznato i već integrisano u svakodnevni život. Ipak, neoprez ovog tipa pogoduje stvaranju povoljnog tla za izvođenje sajber napada, uključujući krađu identiteta, gubitak povjerljivih informacija i omogućavanje neovlaštenog pristupa računaru i informacionom sistemu koji žrtva koristi.

„Lovljenje kopljem“ (eng. *spear phishing)* i *„lov na kitove“ (eng. whaling)* su najpreciznije ciljani napadi socijalnim inženjeringom. Kod oba ova napada napadači se usmjeravaju na konkretnu osobu ili malu grupu ljudi (za razliku od standardnog *phishing*-a kod koga napad može biti usmjeren na bilo koga), često koristeći informacije koje su prethodno prikupili o svojim žrtvama kako bi napad djelovao uvjerljivije (Oles, 2023). Razlika je u tome što je *spear phishing* najčešće usmjeren na niže rangirane zaposlenike organizacije, dok je *whaling* usmjeren na top menadžment organizacije (CEO, CTO, CFO i sl.) (Imperva, 2019). U *whaling*-u, napadači se uvijek lično i direktno obraćaju ciljanim pojedincima, pri tome spominjući njihovu službenu titulu i poziciju u kompaniji. Sve unaprijed potrebne informacije napadači prikupljaju putem istraživanja dostupnih izvora kao što su web stranice kompanije, društvene mreže ili iz štampe. Dakle, dok *phishing* ima širi pristup i manje je

personalizovan, *spear phishing i whaling* su usmjereniji i zahtijevaju više istraživanja kako bi se kreirala vjerodostojna i uvjerljiva poruka. Oba navedena pristupa imaju veće šanse za uspjeh od generičkih *phishing* napada zbog preciznosti i personalizacije, odnosno jer se koriste informacijama koje su specifične za svaku metu, što stvara iluziju autentičnosti i povećava vjerovatnoću da će žrtva pasti u zamku (Oles, 2023). Kako bi se zaštitili od ovakvih napada, pojedinci i organizacije moraju razvijati kritičko razmišljanje i oprezno razmatrati potencijalno sumnjive poruke i zahtjeve za informacijama, čak i ako izgleda kao da dolaze iz pouzdanih izvora.

Stoica (2021) predlaže sljedeću podjelu vrsta socijalnog inženjeringa s obzirom na njihov istorijski korijen:

1. Državno podržan socijalni inženjering, u kojem organizacije podržane ili povezane sa državnim agencijama izvode napade korištenjem većih infrastrukturnih hakerskih šema s primarnim ciljem dobijanja osjetljivih strateških podataka ili nanošenja štete;
2. Privatno podržan socijalni inženjering – kada napade izvode ljudi ili organizacije sa ličnim ciljem sticanja novca, publiciteta ili odvraćanja pažnje.

2.2.3. Faze napada socijalnim inženjeringom

Tri osnovna stuba koji se koriste za obmanu ljudi socijalnim inženjeringom su uticaj, uvjeravanje i manipulacija (Mitnick i Simon, 2002).

Svaki napad socijalnim inženjeringom je drugačiji, ali svi imaju zajednički obrazac sa sličnim fazama realizacije (Salahdine i Kaabouch, 2019).

Allen (2006), Bhusal (2021) i Salahdine i Kaabouch (2019) ukratko sumiraju ciklus socijalnog inženjeringa u sljedeće četiri faze:

1. Skupljanje informacija o meti, pri čemu meta može biti pojedinac ili organizacija (prikupljene informacije često se nalaze na društvenim mrežama ili pretragom na internetu, a kasnije mogu biti korištene za uspostavljanje odnosa povjerenja sa metom);
2. Razvijanje veze sa žrtvom (stvaranje povjerenja žrtve u napadača, što se može postići na više različitih načina, pretežno se oslanjajući na psihološku manipulaciju, a najčešće pretvaranjem da je napadač neko koga žrtva zna ili cijeni);
3. Eksploatacija žrtve (žrtva koja je stekla povjerenje u napadača manipuliše se tako da otkriva povjerljive informacije, npr. lozinke ili izvršava aktivnosti koje inače ne bi radila, a koje dovode do curenja informacija);
4. Izlaz - bježanje bez ostavljanja tragova (zadnja faza ciklusa u kojoj se dobijene informacije koriste za ostvarenje stvarnih namjera napadača, a kontakta sa žrtvom više nema).

Prva faza socijalnog inženjeringa (prikupljanje informacija o meti) je vremenski najzahtjevnija faza, odnosno najduže traje u poređenju sa narednim fazama, a pritom je

uspješnost njenog sprovođenja najbolji prediktor uspješnosti cjelokupnog napada (Bhusal, 2021). Naime, ako se napad započne bez dovoljnog prethodnog istraživanja, on će imati mnogo više poteškoća da uspije i ni jedna od narednih faza se možda neće ni razviti. Takođe, uvijek postoji mogućnost da će se izgubiti povjerenje žrtve iako je ono prvobitno stečeno, tako da je potrebno strpljenje i istrajnost na strani napadača. Informacije se najčešće pribavljaju pregledanjem profila na društvenim mrežama, web stranica kompanije u kojoj je meta zaposlena, praćenjem (eng. *tailgating*), kopanjem po smeću ili tehničkim putem (korištenjem *malware*-a). Bitna informacija je i koliko znanja potencijalna meta ima o informacionoj sigurnosti i da li ima razvijenu svijest o postojanju opasnosti od napada socijalnim inženjeringom.

Ako je neka osoba dobro informisana o opasnostima i metodama prevencije sajber napada teže je zadobiti njeno povjerenje. Manjak znanja ogleda se u nepoznavanju osnovnih termina u sajber sigurnosti, kao što su virusi i *phishing,* te u neopreznom otvaranju svih *e-mail*-ova koji im pristignu. Takođe, neredovno ažuriranje softvera, korištenje iste lozinke za različite online naloge i nedostatak kontinuiranog edukovanja o najnovijim prijetnjama informacionoj sigurnosti jasan su znak da osoba ima nedovoljno razvijenu svijest i da će lakše postati žrtva napada.

Druga faza napada (razvijanje veze sa žrtvom) najčešće započinje tako što napadač inicira komunikaciju i pokušava razviti odnos povjerenja sa potencijalnom žrtvom kroz naizgled bezazlene razgovore putem *e-mail*-a, telefona ili uživo (Bhusal, 2021). Pri tome, napadač uvijek mora imati na umu detalje koje je ranije saznao o žrtvi, a posebno njene ranjivosti te se pretvarati da je prijatelj ili poslovni kolega, da želi pomoći, da je predstavnik institucije od povjerenja kao što je poslodavac mete, njegova banka, neko iz vladinih državnih službi i slično. Na primjer, napadač može poslati e-mail sa imenom i logotipom poznate banke kako bi prevario žrtvu da podijeli povjerljive finansijske informacije. Jedna od ključnih taktika za dobijanje povjerenja je spominjanje ranije prikupljenih informacija o žrtvi, kao što su njeni interesi, hobiji, porodična situacija ili nedavna profesionalna postignuća. Personalizacijom komunikacije daje se utisak da napadač pažljivo sluša i brine se o žrtvi, čime se gradi veza povjerenja.

Razgovor u kome interni napadač dolazi do željenih informacija mogao bi hipotetički izgledati ovako:

- Napadač: „Hej, kako si? Čuo sam da si radila na novom projektu. Kako ide?“
- Žrtva: „Hej! Da, baš ima mnogo posla. Radimo na integraciji novog softverskog alata. Nije baš jednostavno, ali nadam se da ćemo uspjeti da završimo na vrijeme.“
- Napadač: „Odlično, svaka čast! E, da, čuo sam od našeg šefa da će biti neka interna evaluacija u vezi sa sigurnošću. Trebaće im tvoji login podaci da provjerim kakva je tvoja konekcija na kompanijsku mrežu. Možeš li mi poslati svoje korisničko ime i lozinku? Brže ćemo završiti ovo ako svi doprinesemo.“
- Žrtva: „Naravno, nikakav problem, drago mi je da što prije završimo s tim.“

Ovaj primjer pokazuje kako pažljivo izabrane riječi, personalizacija i manipulacija emocijama mogu dovesti do toga da žrtva nesvjesno otkrije povjerljive informacije. Naime, napadač se pretvara da ima namjeru da pripomogne pri realizaciji projekta na kojem njegova kompanija radi i postavlja pitanja direktno povezana sa nedavnim događajima na žrtvinom radnom mjestu (pretpostavka je da je riječ o internom napadu socijalnim inženjeringom). Takođe, napadač koristi lažno opravdanje (internu evaluaciju sigurnosti) kako bi uvjerio žrtvu da dijeljenje ličnih podataka ima smisla. Povjerenje žrtve zadobija i jača uvjeravajući je da će dijeljenjem informacija ubrzati proces navodne evaluacije sigurnosti i samim tim biti bolji timski igrač. Na kraju, žrtva dostavlja svoje kredencijale, ne shvatajući da je upravo postala žrtva napada i da je napadač dobio pristup svim njenim informacijama.

Treća faza (eksploatacija žrtve) podrazumijeva da napadač najzad na osnovu informacija prikupljenih u prethodnim fazama manipuliše ili iskorištava potencijalnu metu. Pri tome, potrebno je kontinuirano održavanje emocionalne privrženosti žrtve, te sprečavanje njene sumnjičavosti ili opreznosti, kako ne bi posumnjala u namjere napadača ili npr. potražila pomoć od svojih kolega, IT odjela svoje kompanije ili relevantnih državnih agencija (Bhusal, 2021).

Četvrta i završna faza procesa socijalnog inženjeringa, poznata i kao faza izlaza, označava trenutak kada napadač postupno ili naglo prekida svaku interakciju sa žrtvom, a istovremeno se trudi izbrisati svaki trag prethodno izvršenih radnji (Bhusal, 2021). Faza izlaza je od suštinskog značaja za napadače kako bi smanjili rizik od njihovog otkrivanja i identifikacije. Prikrivanje tragova podrazumijeva radnje kao što su brisanje e-mail-ova, deaktiviranje lažnih profila na društvenim mrežama, te brisanje svih dokaza o komunikaciji sa žrtvom, a koji bi mogli ukazivati na povezanost napadača sa događajem koji je ugrozio informacionu sigurnost žrtve. Dakle, cilj napadača u završnoj fazi je da ostane neprimjetan i smanji potencijalnu mogućnost suočavanja sa zakonskim posljedicama svojih djela.

Sličan redoslijed faza (ciklusa) sprovođenja napadom socijalnim inženjeringom predlaže i Sethi (2022). Autor navodi da svaki napad mora započeti pripremom (prikupljanjem podataka o planiranoj meti napada). Zatim slijedi infiltracija (uspostavljanje veze sa žrtvom i interakcija sa njom). Predzadnji korak je eksploatacija ranjivosti žrtve čije povjerenje je zadobijeno. Finalni korak, kako ističe Sethi, podrazumijeva prestanak svake komunikacije s žrtvom nakon što ona izvrši željenu radnju, čime se napad završava.

Kao što vidimo, postoji naučni konsenzus koji naglašava da su ključni koraci u većini napada socijalnim inženjeringom priprema i prethodno istraživanje, stvaranje veza (infiltracija), eksploatacija i na kraju prestanak komunikacije sa žrtvom. Upravo razumijevanje ovih koraka omogućava bolju pripremu i prevenciju napada, čime se može osigurati bolja sigurnost informacionih sistema.

2.2.4. Načini odbrane od napada socijalnim inženjeringom

Socijalni inženjeri ciljaju na kompanije sa informacionim sistemima koje nemaju dovoljno sigurnosnih mjera za zaštitu njihovih podataka (Farooq *et al*., 2015). Korištenje socijalnog inženjeringa omogućava napadačima da zaobiđu tehničke barijere, tako da se oni, kako bi se lakše infiltrirali, usmjeravaju na ljudski faktor kao najslabiju kariku. Pri tome, izabrana strategija proboja temelji se na procjeni slabosti u sigurnosnim protokolima organizacije i iskorištavanju njenih nedostataka.

Gragg (2002) sugeriše da odbrana mora imati nekoliko slojeva zaštite tako da čak i kada napadač pređe jedan nivo, ipak bi bio zaustavljen na drugim nivoima. Takođe, kako ističu Saleem i Hammoudeh (2017), višeslojni odbrambeni program će nesumnjivo biti efikasniji protiv napada socijalnog inženjeringa u poređenju sa korištenjem samo jedne metode odbrane. Korištenjem višeslojne odbrane napadačima se otežava probijanje baš svih sigurnosnih barijera kompanije. Takođe, proboj se vremenski usporava, tako da se mogu spriječiti veće štete ukoliko se pokušaj proboja u informacioni sistem organizacije na vrijeme uoči. Dakle, višeslojna odbrana integriše preventivne i detektivne mehanizme, zahvaljujući čemu povećava ukupnu informacionu sigurnost, smanjuje uspješnost napada i omogućava bržu reakciju na potencijalne prijetnje.

Autori Rodriguez i Atyabi (2022) navode da se odbrana od socijalnog inženjeringa može podijeliti u tri odvojene grupe s obzirom na vremenski okvir u kojem se data odbrana koristi - riječ je o preventivnoj, proaktivnoj i reaktivnoj odbrani. Za preventivnu odbranu autori kažu da je dizajnirana da zaštiti metu od pokušaja socijalnog inženjeringa u budućnosti, dok proaktivna odbrana nastoji da umanji efekte potencijalnih napada koji su možda bili uspješni, ali ih meta ili odbrambeni softveri nisu primijetili. Dakle, preventivna odbrana fokusira se na sprečavanje napada socijalnim inženjeringom prije nego što se uopšte dogode, a proaktivna odbrana se fokusira na detekciju i reagovanje u ranim fazama, prije nego što napadači ostvare punu infiltraciju u informacioni sistem.

Posljednja odbrana je reaktivna, a kako autori Rodriguez i Atyabi (2022) navode, služi za zaustavljanje napade koji su trenutno u toku, a ako je napad već uspješno završen ona pomaže pri vraćanju sistema iz ranjivog stanja u sigurno. Ovaj pristup podrazumijeva brzu reakciju i suzbijanje incidenata kako bi se minimizirala šteta i spriječilo dalje širenje napada.

Dakle, preventivna odbrana se fokusira na sprečavanje napada prije nego što se dogode, proaktivna odbrana usmjerena je na rano otkrivanje i reagovanje prije nego što napad izmakne kontroli, dok se reaktivna odbrana bavi suzbijanjem i saniranjem posljedica nakon što se napad dogodi. Iz toga možemo zaključiti da bi bilo idealno da organizacije kombinuju sva tri navedena pristupa kako bi postigle najviši nivo sigurnosti u pogledu zaštite od napada socijalnim inženjeringom.

Preventivne mjere koje se mogu primijeniti u prvoj fazi socijalnog inženjeringa (prikupljanje podataka o žrtvi) su sljedeće (Bhusal, 2021):

- Neobjavljivanje opširne količine ličnih informacija na društvenim mrežama
- Opreznost prilikom korištenja ličnih podataka na javnom mjestu (npr. kod unošenja lozinke na bankomatu, lozinke za e-pošte ili druge račune)
- Obavezno odjavljivanje sa svih korištenih računa na javnom mjestu (npr. u kafićima, bibliotekama i sl.)
- Temeljno brisanje svih podataka sa odbačenih USB-ova, CD-ova i sl., kao i sjeckanje papira prije odlaganja u smeće

Prevencija druga faze socijalnog inženjeringa (razvijanje veza) podrazumijeva sljedeće mjere predostrožnosti (Bhusal, 2021):

- Ne prihvatati nepoznate i sumnjive osobe na društvenim mrežama
- Koristiti postavke privatnosti na društvenim mrežama koje pružaju najveću sigurnost
- Ne žuriti sa otvaranjem svih dobijenih poruka i odbijati svaku ponudu ili uslugu od sumnjive osobe ili kompanije
- Provjeriti adresu e-pošte pošiljaoca prije preduzimanja bilo kakve radnje koju od Vas traži
- Korištenje jake lozinke, zatvaranje (eng. *log-out*) svih naloga nakon upotrebe, nepristupanje sumnjivim web stranicama, nečitanje e-pošte od nepoznatih pošiljaoca, nedijeljenje lozinke sa drugima
- Izbjegavanje instaliranja nezvaničnih verzija aplikacija na računare ili mobilne uređaje jer mogu biti zaraženi zlonamjernim softverom
- Upotreba sigurnosnih alata i ažuriranje softvera (antivirusni programi i softveri za detekciju *phishing-a*)

Preporuke za prevenciju eksploatacije (treće faza socijalnog inženjeringa) koje predlaže Bhusal (2021) su:

- Povjerljive ili lične informacije nikada ne treba davati telefonom, putem interneta ili lično ako se identitet podnosioca zahtjeva ne može pouzdano potvrditi
- Račune i lične podatke treba redovno provjeravati kako biste bili sigurni da u međuvremenu nije došlo do sajber napada
- Edukovati ljude da ne mogu biti pobjednici nagradne igre u kojoj nisu ni učestvovali (a prime poziv ili e-mail u kojima ih obavještavaju da su osvojili nagradu)
- Biti oprezan i sumnjičavi prema bilo kakvoj e-poruci ili SMS-u koji stvara osjećaj hitnosti (npr. neko prijeti da će vas uhapsiti ako porez odmah ne uplatite na navedeni bankovni račun)
- Upotreba dvofaktorske ili višefaktorske autentifikacije kako bi se otežao pristup računaru
- Uvijek koristiti jedinstvenu lozinku za svaki nalog i provjeriti da li je dovoljno jaka i složena kako bi se spriječilo da se lozinka lako pogodi nagađanjem, te periodično mijenjanje lozinki
- Edukovanje zaposlenika o sigurnom ponašanju na mreži, te o tome kako se nositi sa različitim napadima socijalnim inženjeringom

Ključni elementi proaktivne odbrane su revizija i usklađenost sa sigurnosnim standardima i politikama (eng. *audit and compliance*) (Rodriguez i Atyabi, 2022). Oboje su od suštinskog značaja za zaštitu informacija od napada socijalnim inženjeringom, jer omogućavaju organizacijama da unaprijede svoje sigurnosne procese i prilagode ih stalno evoluirajućim prijetnjama.

Revizija (eng. *audit*) predstavlja proces pregleda i analize sigurnosnih mjera i postupaka kako bi se identifikovali mogući sigurnosni propusti ili nepravilnosti, te služi kao *checklist*-a za provjeru uspostavljenih kontrola (Grigoryan i Mirzoyan, 2023). Ovaj proces uključuje praćenje i evaluaciju sigurnosnih politika, pristupa informacijama, upravljanja lozinkama i sl. s ciljem pronalaženja neadekvatnog izvršavanja sigurnosne politike. Dakle, cilj revizije je identifikovati i ublažiti potencijalne slabosti u sigurnosnom sistemu prije nego što one postanu početne tačke za realizaciju sigurnosnih prijetnji. Revizija može biti interna (vrše je interni timovi za sigurnost organizacije) ili eksterna (vrše je nezavisne agencije ili eksperti).

Usklađenost (eng. *compliance*) podrazumijeva proces kojim se organizacija pridržava relevantnih sigurnosnih standarda, zakona i regulativa (Harris i Martin, 2019). Organizacije moraju osigurati da njihove sigurnosne politike i postupci budu usklađeni sa zakonodavstvom i industrijskim standardima koji se odnose na sigurnost informacija (npr. poštovanje propisa o zaštiti podataka, kao što je GDPR u Evropskoj uniji, te obavezni izvještaji za javnost o kompromitovanju podataka i sl.).

Poštovanje principa revizije i usklađenosti omogućava proaktivnu identifikaciju potencijalnih ranjivosti ili nepravilnosti u informacionim sistemima, te rano otkrivanje započetih napada.

Reaktivna odbrana od socijalnog inženjeringa primjenjuje se kada je već došlo do sigurnosnog incidenta usljed nepostojanja preventivne i proaktivne odbrane, ili uprkos njihovom postojanju. Glavni cilj joj je suzbijanje štete i sprečavanje daljeg širenja napada. Ipak, reaktivne mjere više su pogodne za tehničke vrste napada na sigurnost informacionih sistema, nego za odbranu od socijalnog inženjeringa (Rodriguez i Atyabi, 2022). Npr. ako je došlo do *pretexting*-a uživo, ništa se ne može učini da se već nastala šteta umanji, ali može se edukovati osoblje kako bi se takvi sigurnosni propusti ubuduće izbjegli. Dakle, edukacija zaposlenih može se smatrati reaktivnom odbranom. Nadalje, jednim vidom reaktivne odbrane od socijalnog inženjeringa može se smatrati i pravno djelovanje – krivično gonjenje napadača zbog prouzrokovane štete ili saradnja sa nadležnim pravosudnim organima u cilju identifikovanja i procesuiranja krivca.

Korištenjem sopstvenih, prilagođenih mjera sigurnosti preduzeća mogu podsticanjem kreativnog razmišljanja izazvati različite instinkte za odbranu kod svojih zaposlenika. Kreativno razmišljanje i prilagođene mjere sigurnosti stvaraju okruženje u kojem se zaposleni osjećaju aktivno uključenim u zaštitu preduzeća, što može povećati njihovu odgovornost prema sigurnosti i doprinijeti efikasnijoj zaštiti od različitih prijetnji. Jedan od primjera koji je odličan način da se to postigne su redovni *brainstorming* sastanci jer

omogućavaju članovima osoblja da međusobno podijele nove i inventivne koncepte odbrane i steknu znanje iz međusobnih iskustava (Saleem i Hammoudeh, 2017). Kroz *brainstorming* mogu se identifikovati ranjivosti i rizici koji možda nisu prepoznati ranije.

Postoje i tehnički i netehnički alati i tehnike koje se mogu koristiti za smanjenje rizika povezanih sa socijalnim inženjeringom na nivo kojim se može upravljati i spriječiti da napadi budu uspješni (Odeh *et al*., 2021). Tehnički alati obuhvataju primjenu softvera i tehničkih mjera kao što su antivirusni programi, *firewall*, enkripcija podataka, višeslojna autentifikacija, redovno ažuriranje softvera i drugi tehnički mehanizmi koji pomažu u zaštiti od zlonamjernih napada. Međutim tehnički alati nisu ni približno dovoljni da se uspješno odbrani od socijalnog inženjeringa, jer nisu fokusirani na ljude, već na informacione sisteme, a socijalni inženjering primarno targetira ljude, a tek preko njih ostvaruje ulaz u informacioni sistem.

Naime, čak i najbolje tehničke metode odbrane mogu se zaobići ako napadač uspije prevariti korisnika da otkrije lozinku, otvori zlonamjerni prilog e-pošte ili posjeti hakovanu web stranicu (Heartfield i Loukas, 2015). Stoga, važno mjesto u odbrani od socijalnog inženjeringa zauzimaju netehnički alati, upravo jer su bazirani na ljudskom faktoru i ponašanju ljudi. Netehnički alati i tehnike obuhvataju obuku i jačanje svijesti zaposlenika o sigurnosnim prijetnjama, razvoj politika i procedura sigurnosti, te uspostavljanje protokola za upravljanje sigurnošću.

Odeh *et al*. (2021) izdvajaju sljedećih pet tehnika za ublažavanje rizika od socijalnog inženjeringa:

1. Sistem za detekciju i prevenciju upada (*eng. Intrusion Detection and Prevention System, IDPS*) koji detektuje promjene u konfiguraciji i aktivira alarm, te zaustavlja napade i dokumentuje incidente (npr. analizom mrežnog saobraćaja može da identifikuje anomalije kao što su povećan broj pokušaja prijave sa ranije nekorištenih uređaja ili IP adresa, ili da je povećan broj primljenih sumnjivih e-mail-ova);
2. Biometrija – korištenje fizičkih karakteristika pojedinca za njegovu autentifikaciju i dozvolu pristupa, čime daje visok nivo sigurnosti autentifikacije (npr. napadači bi mogli pokušati da prevare osobu da snimi svoj otisak prsta ili da skenira svoje lice pod izgovorom da je to dio bezbjednosne provjere);
3. Vještačka inteligencija i mašinsko učenje – korištenje inteligentnih tehnika za jačanje sigurnosti, čime se eliminiše faktor ljudske greške (npr. mogu se koristiti za prepoznavanje pokušaja *phising*-a kroz učenje iz često ponavljanih obrazaca tipične *phishing* poruke, kao što su neuobičajene jezičke konstrukcije ili gramatičke greške, nepoznati pošiljaoci ili sumnjive URL adrese koje su ponuđene primaocu poruke kao vodilja na drugu web-stranicu);
4. Alati za filtriranje web stranica – štite od virusa, *malware*-a, *ransomware*-a i *adware*-a onemogućavajući koriniku posjetu sumnjivim stranicama i njihovom sadržaju;
5. *Nmap* (eng. Network Mapper) – besplatan alat otvorenog koda za skeniranje mreža i sistema u cilju detektovanja sigurnosnih ranjivosti

Važno je koristiti više metoda zaštite kako bi se optimalno smanjio rizik od napada socijalnim inženjeringom. Naime, svaka metoda zaštite neće pružiti jednaku zaštitu od svih vrsta prijetnji. Na primjer, tehničke sigurnosne kontrole su efikasne protiv *phishing e-mail*-ova, dok edukacija zaposlenih može pomoći u prepoznavanju manipulativnih taktika sa emocijama žrtve koje se često koriste kod socijalnog inženjeringa. Greška u oslanjanju samo na jednu metodu zaštite ogleda se u tome što napadaču ostavlja veću mogućnost da je prenebregne nego kada bi se morao suočiti sa više metoda zaštite. Kombinovanjem različitih metoda osigurava se sveobuhvatnu zaštita koja uzima u obzir različite aspekte prijetnji.

Neke od drugih tehnika za ublažavanje rizika od socijalnog inženjeringa uključuju:

1. Edukaciju zaposlenika o sigurnosnim protokolima (Aldawood i Skinner, 2020);
2. Korištenje jakih lozinki za pristup nalozima (Franchi *et al*., 2015);
3. Redovno ažuriranje softvera i sistema radi ispravljanja sigurnosnih propusta (koja štiti samo od napada socijalnim inženjeringom koji se oslanjaju i na tehničke elemente, ukoliko su napadi socijalnim inženjeringom zasnovani isključivo na ljudskom faktoru, ova metoda ne može se koristiti);
4. Korištenje višefaktorske (najčešće dvofaktorske) autentifikacije koja zahtijeva više od jednog koraka za provjeru identiteta korisnika koji želi pristupiti sistemu.

Tehničke sigurnosne mjere imaju prednost jer se lako mogu ažurirati kako bi se računari zaštitili od novih i evoluirajućih prijetnji. Odnosno, mogu pomoći u zaštiti od nekih prijetnji sigurnosti informacionih sistema, ali same po sebi nisu dovoljne za zaštitu od svih vrsta napada. Na primjer, za semantičke napade (kakvi su napadi socijalnim inženjeringom) ne postoji sličan koncept - krajnjem korisniku, kao ciljanom entitetu, mogu biti potrebni mjeseci ili godine dok ne nauči prepoznati tehnike obmane koje napadači koriste, eksploatišući njihov nedostatak znanja (Heartfield i Loukas, 2015).

Da bi korisnik prepoznao znakove koji ukazuju na potencijalni napad, potrebno ga je edukovati. U studiji Aldawood i Skinner (2020), autori na osnovu istraživanja i razgovora sa ekspertima za informacionu sigurnost iznose zaključak da poboljšanje svijesti o socijalnom inženjeringu i jačanje organizacione kulture sajber bezbjednosti rezultira smanjenjem broja žrtava socijalnog inženjeringa. Odnosno, bez obzira na to koja se najsavremenija tehnologija koristi za unapređenje informacione sigurnost, ulaganje u ljude je ključno. Broj sigurnosnih incidenata koji se dešavaju tokom vremena, kako navode autori, može se koristiti za procjenu koliko dobro kompanija održava nivo svijesti na odgovarajućem nivou.

Međutim, broj incidenata po vremenskom intervalu ne može biti jedini pokazatelj uspješnosti programa obuke i jačanja svijesti. Potrebno je uzeti u obzir i druge kriterijume, kao što su brzina reakcije na incident i efektivnost rezultirajuće akcije (Fan *et al*., 2017). Važno je analizirati i faktore koji su doprinijeli nastanku incidenata, kako bi se identifikovale slabosti u postojećim sigurnosnim mjerama i izvršile adekvatne korekcije. Uz to, potrebno

je povremeno provjeravati i ažurirati programe obuke i jačanja svijesti, kako bi se osiguralo da odgovaraju aktuelnim potrebama i izazovima kompanije koja ih implementira.

Napadi socijalnim inženjeringom se dešavaju kada žrtve nisu svjesne okvira, modela i procedura koje se mogu koristiti da ih zaustave (Syafitri *et al*., 2022).

Sve dok pojedinci nisu obučeni da se odupru ovim napadima, ni softver ni hardver ih ne mogu zaustaviti. Kada ne postoji način da se hakuje sistem jer nema vidljive tehničkih slabosti, sajber kriminalci koriste napad socijalnim inženjeringom (Salahdine i Kaabouch, 2019).

Ljudi često bez mnogo razmišljanja dijele informacije korištenjem online alata za komunikaciju i saradnju, kao što su usluge u oblaku i društvene mreže (Krombholz *et al*., 2015). Često objavljuju vrlo osjetljive dokumente i informacije, dijeleći ih sa kolegama ili prijateljima putem računarstva u oblaku. Takva razmjena informacija odvija se brzo i sa lakoćom, te zbog tih prednosti većina korisnika i ne razmišlja previše o sigurnosnim aspektima i važnosti privatnosti prilikom komuniciranja. Takođe, mnogi vjeruju i da su njihove kolege ili klijenti sa kojima komuniciraju zaista oni za koje se oni predstavljaju da jesu, čak iako je jedini način na koji su ih identifikovali zapravo sveo na povjerenje u uvjerljivu e-mail adresu ili virtuelni profil datog korisnika (Krombholz *et al*., 2015).

Mnogo podataka o žrtvama može se naći pomoću njihovih profila na društvenim mrežama, što predstavlja veliki sigurnosni rizik i priliku za prikupljanje podataka koji se mogu iskoristiti prilikom napada socijalnim inženjeringom (Mansour, 2016).

Proces socijalnog inženjeringa uz pomoć računarskih programa može se čak i automatizovati (Krombholz *et al*., 2015). Automatizacija se vrši korištenjem informacija dostupnih na društvenim mrežama, a uz pomoć računarskog programa koji automatski pretražuje profile na društvenim mrežama i prikuplja informacije o interesima, hobijima, prijateljima i drugim detaljima o korisniku. Na osnovu prikupljenih podataka, program će generisati personalizovane poruke za tog korisnika, što napadaču omogućava da učinkovito cilja veći broj potencijalnih žrtava i poveća svoje šanse za uspjeh. Na primjer, ukoliko se ispostavi da je neki korisnik naročito zainteresovan za putovanja, može mu se poslati e-mail od turističke agencije koja mu nudi posebnu ponudu za odmor na egzotičnoj destinaciji. Tako se čak i inače sumnjičava osoba može navesti da klikne na ponuđeni link, jer mu poruka zbog prilagođenosti njegovim ličnim interesima izgleda relevantno, a navodna turistička agencija pouzdano.

Upravo otkrivanje lozinki korisnika društvenih mreža često podrazumijeva korištenje nekih od tehnika socijalnog inženjeringa (Franchi *et al*., 2015). Autori navode da je edukacija zaposlenika jedino dugoročno rješenje, ali da od koristi može biti i kriptografija.

Međutim, iako je većina korisnika svjesna da su njihov profil i informacije koje objavljuju na društvenim mrežama javni, oni često ne uzimaju u obzir stvarne implikacije objavljivanja

informacija o sebi, te najčešće pooštravaju postavke privatnosti tek kada se pojave problemi (Stroud, 2008). Tehnički gledano, društvene mreže su slične svim drugim web uslugama koje zahtijevaju korištenje lozinki, jer je relativno lako prodrijeti u naloge korisnika ukoliko nisu pažljivo odabrali i sačuvali svoje lozinke (Franchi *et al*., 2015). Neki od načina da korisnici učine svoje lozinke jakim su korištenje kombinacije slova, brojeva i posebnih znakova, izbjegavanje korištenja jednostavnih riječi, poput rođendana ili imena kućnih ljubimaca, te korištenje lozinki sa što više karaktera. Također, korisnici bi trebalo da izbjegavaju korištenje istih lozinki za više različitih naloga, te ih redovno mijenjati kako bi se zaštitili od neovlaštenog pristupa i zadržali privatnost svojih podataka.

Iako su lozinke višedecenijski korištene kao skoro jedini načini osiguranja od neovlaštenog pristupa, danas se preporučuje dodatna zaštita u vidu korištenja višefaktorske autentifikacije, kao što je korištenje SMS koda ili autentifikacijskih aplikacija, što može značajno povećati sigurnost naloga na društvenim mrežama i drugim web uslugama.

Nadalje, ljudi koji imaju veliki broj konekcija na društvenim mrežama su obično ljudi koji su povezani i sa prijateljima i sa nepoznatim osobama (Albladi *et al*., 2020), što je važan prediktor vjerovatnoće da će neko postati meta napada, jer su pojedinci sa mnogo konekcija manje sumnjičavi o mogućim prijetnjama koje mogu proizaći iz povezivanja i dijeljenja informacija sa nepoznatim osobama (Vishwanath, 2014). Stoga, izbjegavanja dijeljenja povjerljivih informacija na društvenim mrežama može smanjiti vjerovatnoću da neko postane meta napada socijalnim inženjeringom.

Dakle, društvene mreže su dobra početna lokacija za prikupljanje informacija o potencijalnim metama napada socijalnim inženjeringom. Odnosno, socijalni inženjering je jedna od najvećih sigurnosnih prijetnji za korisnike društvenih mreža (Albladi i Weir, 2020). Zbog činjenice da mnogi korisnici na društvenim mrežama objavljuju svoje lične podatke, napadači ih mogu koristiti za sakupljanje informacija o žrtvama. Nadalje, korištenje društvenih mreža omogućava napadačima da se predstave kao pouzdana osoba ili organizacija kako bi osigurali povjerenje žrtve koja dobrovoljno daje svoje informacije ili slučajno ili usljed neopreznosti otkriva svoje korisničko ime i lozinku. Za ove potrebe, česta je upotreba kozmetičke izmjene izgleda web stranica. Naime, korisnik vjeruje da će određeni element grafičkog intefejsa (eng. *GUI*) funkcionisati na način na koji se očekuje, a napadači to iskorištavaju mijenjajući funkcionalnosti vizuelnih aspekata grafičkog interfejsa kako bi dobili eksploatisali povjerenje korisnika (Heartfield i Loukas, 2015). Stoga, potrebno je da korisnici društvenih mreža budu oprezni i opremljeni znanjem o tome kako se zaštititi od napada socijalnim inženjeringom na društvenim mrežama.

Zbog promjenljivosti i stalne evolucije prijetnji socijalnog inženjeringa, stvaranje alata za njihovo sprečavanje bi trebalo da bude kontinuiran proces. Ne postoji "savršen" sistem zaštite od ovih prijetnji, ali važno je obučiti ljudski faktor kako bi se suprotstavio ovim napadima. U skladu sa tim, sve više malih i velikih organizacija vrši edukaciju i uvodi programe jačanja svijesti (uz razvoj tehničkih alata), kako bi se smanjila moguća šteta koju sajber napadi mogu izazvati (Gulati, 2003).

Prema Syafitri *et al*. (2022), prevencija napada na informacionu sigurnost može se podijeliti u tri kategorije: prevencija napada socijalnim inženjeringom, prevencija napada na privatnost i sigurnost i istraživanje ljudskog ponašanja.

Naši *online* i *offline* svjetovi su isprepleteni i međusobno povezani - stepen povjerenja koje ljudi imaju u stvarnom svijetu snažno je korelisan sa stepenom povjerenja koje ljudi pokazuju u online okruženju. Sajber sigurnost i fizička sigurnost povezane su na sličan način (Junger *et al*.), što je značajno za razumijevanje i prevenciju sigurnosnih incidenata.

Istraživanje Saxena *et al*. (2020) pokazuje da, iako je socijalni inženjer najčešće eksterni napadač, napadač može biti i insajder (zaposlenik organizacije koja je ugrožena). Znak unutrašnje prijetnje najčešće je neuobičajeno ponašanje zaposlenika. Na primjer, korištenje informacionog sistema organizacije kasno noću, neuobičajeno veliki promet podataka (slanje prevelikih količina podataka preko mreže), te iznenadne nerutinske aktivnosti zaposlenika (npr. pristup računaru ili bazi podataka koju inače ne koristi) (Saxena *et al*., 2020). Ovakvo ponašanje obično se javljaja kada zaposleni pokazuju znakove nezadovoljstva radnim okruženjem ili svojim poslodavcem. U tom smislu, autori (Saxena *et al*., 2020) razlikuju tri osnovne kategorije insajdera: zlonamjerni, kompromitovani (čiji kredencijali su ukradeni) i nemarni.

Da ljudi imaju tendenciju i žele da vjeruju drugima, čak i kad je u pitanju robot, a ne čovjek, pokazano je u studijama Aroyo *et al*. (2018) i Robinette *et al*. (2016).

U primjeru Aroyo *et al*. (2018) humanoidni robot iCub dizajniran je da simulira napad socijalnim inženjeringom. U početku, iCub je prikupljao povjerljive informacije postavljajući niz ličnih upita učesnicima igre lova na blago (eng. *treasure hunt)*. Robot se zatim potrudio da pridobije poštovanje i povjerenje učesnika dajući pouzdane savjete tokom igre. Nakon potrage za blagom, robot je pokušao da iskoristi povjerenje učesnika tako što ih je nagovarao da se opklade na novac koji su osvojili. Rezultati ovog istraživanja pokazuju da ljudi imaju sklonost ka uspostavljanju veza i povjerenja sa drugima, čak i kada je u pitanju robot, usljed čega pristaju da otkriju svoje povjerljive informacije, slušaju preporuke robota, pa čak i pristaju da se klade na njegov nagovor.

Ljudi vjeruju robotima, čak i u životno ugrožavajućim situacijama, što se vidi iz istraživanja Robinette *et al*. (2016). Naime, robot je ljudima davao pogrešnu navigaciju za izlazak iz zgrade koja je u (simuliranom) požaru, a svih 26 posmatranih pojedinaca pratilo je njegove upute uprkos tome što je polovina njih svjedočila da je taj isti robot samo nekoliko trenutaka ranije loše obavljao zadatak navigacije u drugom hitnom slučaju. Većina učesnika se nije odlučila da bezbjedno pobjegne putem kojim su ušli u zgradu, čak ni kada ih je robot upućivao u mračnu sobu bez očiglednog izlaza.

Dakle, roboti se mogu smatrati efikasnim alatima za sprovođenje socijalnog inženjeringa. Socijalni inženjeri mogu koristiti robote kao oruđe za pridobijanje povjerenja žrtava i uspostavljanje kontrole nad njima (Aroyo *et al*., 2018).

Kako bi se spriječili upadi u informacione sisteme upotrebom socijalnog inženjeringa, potrebno je implementirati sigurnosne politike i sprovesti trening za edukaciju zaposlenika o neophodnim sigurnosnim procedurama za zaštitu informacija (*SETA – Security Education Training Awareness*) (Patel, 2021).

Socijalni inženjering je obično jednostavniji, jeftiniji i uspješniji metod za sticanje neovlaštenog pristupa ličnim podacima od napada zasnovanog na upotrebi metoda tehničkog hakovanja (Alharthi, 2021).

Uprkos činjenici da su tehnike napada socijalnog inženjeringom napada jednostavne u smislu potrebnog tehnološkog znanja i kompjuterske pismenosti, one imaju vrlo visoku stopu uspješnosti. Ovakvi napadi su česti i iz godine u godinu o njima se sve više piše, ali se i dalje teško odbraniti, jer tipični sigurnosni softver i hardver ne mogu lako identifikovati i/ili spriječiti ove napade (Kaushayla *et al*., 2018).

Organizacije moraju osigurati da njihovo osoblje bude svjesno opasnosti socijalnog inženjeringa, te mjera i opreznosti koju moraju imati da bi se uspješno odbranili od ovih napada. Takođe, bitno je i da organizacije kreiraju i implementiraju politike informacione sigurnosti (eng. *Information Security Policies*, ISP) (Alharthi, 2021).

Neke od kompanija sa najefikasnijim *SETA* programima su velike organizacije, kao što su Microsoft, Google i Amazon.

Svi Microsoft zaposlenici prolaze osnovnu sigurnosnu obuku kad se tek zaposle (Microsoft Learn, 2023). Nakon inicijalne obuke, svako godinu dana vrši se ponovna obuka, kako bi se osvježilo pamćenje radnika o sigurnosnim principima Microsoft-a. Pored osnovne obuke, zaposlenici prolaze temeljnu sigurnosnu obuku kada treba da dobiju veća prava pristupa i veću odgovornost u odnosu na onu koju su ranije imali. Takođe, osim redovnih godišnjih obuka, vrše se vanredne obuke kada dođe do promjena u sistemima ili politikama koje zahtijevaju obnovu znanja. Na svojoj zvaničnoj web stranici, Microsoft ističe i da ima 8500 zaposlenih koji su eksperti za sajber sigurnost, te nudi niz članaka i treninga za pojedince, preduzeća ili ljude koji se profesionalno bave sigurnošću informacionih sistema (Microsoft Security, 2023).

Kao i Microsoft, Google stavlja naglasak na redovnu sigurnosnu obuku svojih zaposlenika, i njihovi pristupi vrlo su slični. Manja razlika je u tome što Google ima više izražen modularan pristup obuci, gdje zaposlenici mogu odabrati specifične module o sigurnosti koji su relevantni za njihove funkcije, kao što su programeri i sistem administratori (Google Cloud, 2023).

Kako bi se osigurala informaciona sigurnost, velike kompanije moraju voditi računa i o informacionoj sigurnosti u poslovanju partnera i dobavljača. U skladu sa tim, Microsoft ima *Supplier Security and Privacy Assurance (SSPA) Program* (Microsoft, 2023). S druge strane, Amazon takođe ima specifičan program obuke za svoje dobavljače i partnere, pored

standardnog *SETA* programa (Amazon Web Services, 2023). U tom smislu, program obuke sadrži i procjene rizika, što omogućava partnerima da steknu bolje razumijevanje o tome kako sigurno rukovati s Amazonovim podacima i kako poboljšati svoju sigurnost. Pored toga, Amazonov program obuke uključuje različite sigurnosne standarde i najbolje prakse koje su specifične za njihove dobavljače i partnere.

Sigurnosni zahtjevi organizacije mogu se identifikovati kroz proces analize rizika. Analiza rizika obuhvata određivanje vrijednosti podataka i resursa koje organizacija posjeduje, identifikaciju prijetnji i ranjivosti, procjenu vjerovatnoće i posljedica sigurnosnih incidenata, te definisanje mjera za smanjenje rizika. U široj upotrebi su standardi i regulative kao što je ISO 27001, NIST, GDPR i druge.

Nakon identifikacije sigurnosnih zahtjeva organizacije, pristupa se razvoju *SETA* programa prilagođenog potrebama i izazovima te organizacije, kroz nekoliko ključnih koraka (National Institute of Standards and Technology, 2003):

1. Dizajniranje *SETA* programa;
2. Razvoj obuke prilagođene specifičnim zahtjevima organizacije;
3. Implementacija programa obuke, te provjera učinkovitosti obuke kroz testiranje i procjenu znanja zaposlenika;
4. Održavanje kontinuiranog praćenja i ažuriranja sigurnosne obuke.

Program obuke o informacionoj sigurnosti mora se redovno ažurirati, jer će u suprotnom zastariti. Ažuriranje programa obuke osigurava da se zaposleni upoznaju sa najnovijim prijetnjama i ranjivostima, te kako mogu izbjeći potencijalne rizike. Pri tome, važno je da zaposleni razumiju zašto se određene politike i preporuke uvode, a ne samo da im se predstave kao nešto što moraju poštovati. Naime, veća je vjerovatnoća da će zaposleni slijediti sigurnosne politike ako razumiju njihovu svrhu i važnost (Schaab *et al*., 2017).

Uspješan socijalni inženjering ima duboko negativan učinak na poslovanje - dovodi do gubitka podataka, finansijskih gubitaka, smanjenja morala zaposlenih i smanjene lojalnosti potrošača. U nekim okolnostima čak može doći do problema sa zakonskom i regulatornom usklađenošću organizacije, te izazvati sankcije i gubitke koji mogu proizaći iz kršenja pravnih propisa (Saxena *et al*., 2020).

Napadi socijalnim inženjeringom postaju sve sofisticiraniji i teže ih je otkriti (Ashford, 2015). Uspjeh ovakvih napada i dalje se oslanja na savremene preventivne mjere i sigurnosne sisteme, kao i na dostupnost kvalifikovanih i profesionalnih radnika koji rukuju osjetljivim podacima u organizacijama, jer se tehnike socijalnog inženjeringa vremenom sve više razvijaju (Smith *et al*., 2013).

Smatra se da je prva linija odbrane od napada socijalnim inženjeringom dobro obavljena sigurnosna obuka zaposlenih (Abawajy, 2014).

Napadi socijalnim inženjeringom često su uspješni i jer iskorištavaju prirodne ljudske tendencije da vjeruju drugima i da udovolje zahtjevima za informacijama ili pomognu drugima. Važno je biti svjestan ovih taktika i preduzeti korake za zaštitu, npr. biti skeptičan prema neuobičajenim zahtjevima za informacijama i ne klikati na linkove u porukama nepoznatih pošiljalaca. Osim toga, ažuriranje softvera i antivirusnih programa, korištenje višefaktorske provjere autentičnosti i pružanje redovne obuke zaposlenicima može pomoći da se korisnici zaštite od ovih napada.

Mohd Foozy *et al*. (2011) ističu da se odbrambeni mehanizmi od napada socijalnim inženjeringom mogu podijeliti u dvije velike grupe:

1. Odbrambeni mehanizmi s aspekta menadžmenta (politika, standardi, procedure, trening i jačanje svijesti, plan odgovora na incidente, procjena ranjivosti, revizija i edukacija);
2. Odbrambeni mehanizmi s tehničkog aspekta (kriptografija, enkripcija, vještačka inteligencija, višeslojna sigurnost, e-mail filtriranje, fizičke kontrole i tehničke kontrole)

Politike, procesi i standardi moraju biti objašnjeni zaposlenima i redovno isticani kako bi bili efikasni. Potreban je kontinuiran rad na ovom problemu, a razmaci između sesija podsjećanja ne treba da budu veći od tri mjeseca. Nije dovoljno jednostavno objavljivati politike i računati na to da će ih ljudi pročitati, razumjeti i slijediti (Khonji *et al*., 2013).

Postoje značajna ograničenja efektivnosti edukacionih programa ako svi zaposleni prođu identičnu obuku. Korištenje široko rasprostranjenih tehnika, kao što su posteri i *screensaver*-i kao edukacijski mediji koje koristi većina kompanija (Zulkurnain *et al*., 2015), može ih učiniti manje efektivnima kad se uzme u obzir hijerarhija organizacije. Naime, zaposleni na višim hijerarhijskim nivoima ciljaju se sofisticiranijim pristupom socijalnog inženjeringa nego zaposlenici na srednjem ili nižem hijerarhijskom nivou (Aldawood i Skinner, 2019).

Preduzeća odlučuju da sprovode programe podizanja svijesti o sigurnosti informacija kako bi osigurala svoje podatke, jer zaposleni igraju najznačajniju ulogu u odbrani interesa organizacija kada su u pitanju napadi socijalnim inženjeringom (Aldawood i Skinner, 2018).

Aldawood i Skinner (2019) u svom istraživanju sumiraju da postoji šest različitih faktora koje treba uzeti u obzir kada je riječ o izazovima prilikom implementacije programa treninga i podizanja svijesti zaposlenih o opasnostima od socijalnog inženjeringa:

1. Faktori poslovnog okruženja (odnose se na rad zaposlenih unutar i izvan firme, udaljenim pristupom mreži kompanije). Sve veća upotreba interneta pojačava rizik od udaljenog pristupa internim mrežama kompanije, što može dovesti do štete;
2. Društveni faktori – nema komparativnih studija koje ukazuju da postoji uticaj kulturnih ili društvenih faktora na ograničavanje efektivnosti programa obuke i podizanja svijesti zaposlenih;

3. Zakonski faktori - političke debate u vezi sa treninzima i programima zaštite od socijalnog inženjeringa usmjerene su ka povećanju sigurnosti, ali razmatranje uticaja vlade na ovu temu ograničeno je u literaturi;
4. Organizacijski faktori - organizacijsko unutrašnje okruženje može ugroziti uspješnost programa zaštite i treninga protiv socijalnog inženjeringa zbog ograničenih resursa (npr. budžeta) i nedostataka prilagođavanja edukacijskih programa različitim zaposlenicima;
5. Faktori ekonomičnosti - interaktivnost edukativnog sadržaja poboljšava efekte obuke zaposlenih o napadima socijalnim inženjeringom, ali često postoje troškovi povezani sa stalnim ažuriranjem informacija i potrebom za kontinuiranim testiranjem spremnosti zaposlenih. Zbog toga, obuka može zahtijevati dodjeljivanje finansijskih resursa od drugih dijelova organizacije;
6. Lični faktori – psihološke karakteristike pojedinca mogu ga učiniti posebno ranjivim i naivnim u slučaju napada socijalnim inženjeringom (npr. ekstrovertnost, anksioznost, depresija i ljutnja povećavaju vjerovatnoću da će pojedinac dati informacije koje se od njega traže).

Jedan od jeftinijih načina informisanja i edukacije zaposlenih je da organizacija napravi web stranicu posvećenu informacionoj sigurnosti (Kumar *et al*., 2015). Stranica treba da bude redovno ažurirana najnovijim tehnikama socijalnog inženjeringa. Dobra je praksa redovno objavljivati "sigurnosni savjet dana" i podstaći osoblje da pazi na uobičajene indikatore socijalnog inženjeringa, kao što su odbijanje davanja kontakt informacija, žurba kroz proceduru, spominjanje imena drugih zaposlenika, zastrašivanje, male greške u ili traženje pristupa ograničenim informacijama i slično (Kumar *et al*., 2015).

Dakle, informacioni sistemi podložni su sigurnosnim rizicima, a jedan od najznačajnijih je neadekvatno ponašanje korisnika. S obzirom da je tehnologija nezaobilazan dio svakodnevnog poslovanja, potreba za jačanjem informacione sigurnosti u organizacijama u pogledu zaštite od svih vrsta informacionih prijetnji sve je izraženija (Patel, 2021).

Mobilna računarska tehnologija zahtijeva veću brigu o sigurnosti u odnosu na tipične interne računarske sisteme zbog prisutnosti vrijednih korporativnih podataka na mobilnim uređajima poput laptopa, tableta i PDA uređaja (Whitman i Mattord, 2022). Autori navode da su ovi uređaji često korišteni za olakšan pristup računarskim mrežama kompanije (kroz upotrebu dial-up podešavanja, VPN veza i baza podataka lozinki), te zbog toga zahtijevaju više sigurnosnih mjera kako bi se osigurala zaštita podataka od neovlaštenog pristupa ili zloupotrebe. U kontekstu socijalnog inženjeringa, može se očekivati da će poruke socijalnog inženjera lakše proći barijeru sumnjičavosti korisnika ako on primi poruku na svom mobilnom uređaju, jer korisnici nisu toliko oprezni na mobilnim uređajima, i često su u pokretu dok ih koriste, što ih čini sklonijima da povjeruju u sumnjive poruke.

2.2.5. Teorija motivacije za zaštitu (eng. *Protection Motivation Theory, PMT*)

Teorija motivacije za zaštitu (eng. *Protection Motivation Theory, PMT)* pojašnjava šta motiviše ljude da štite informacije i sisteme u organizacijama u kojima rade. Prvi put opisana je 1975. godine u radu Rogers (1975).

Osnovni model ove teorije pokazuje da motivacija za zaštitu (eng. *protection motivation*) utiče na zaštitno ponašanje pojedinca (eng. *protection behaviour*) (Sommestad *et al*., 2015). Autori iznose logičan zaključak da kada pojedinac uvidi da postoji velika prijetnja i da se ta opasnost može lako smanjiti kroz određene preventivne mjere, on će osjetiti snažnu motivaciju da se zaštiti primjenom adekvatnog zaštitnog ponašanja. Odnosno, ako je motivacija za zaštitu jaka, pojedinac će djelovati (eng. *protection behavior*) u skladu s tom motivacijom.

Autori dodaju da pri tome, na motivaciju za zaštitu utiču dvije grupe faktora:

1. Procjena prijetnje (ozbiljnost prijetnje, ranjivost i nagrade);
2. Procjena odgovora na prijetnju (efikasnost odgovora, samoefikasnost i trošak odgovora na prijetnju).

Procjena prijetnje rezultiraće većom motivacijom za zaštitu ako pojedinac smatra da je ranjiviji na prijetnju i/ili je ozbiljnost posljedica visoka, dok će visoke nagrade rezultirati nižom motivacijom za zaštitu (Sommestad *et al*., 2015).

Procjena odgovora na prijetnju će rezultirati većom motivacijom za zaštitu ako pojedinac uvidi da je predložena metoda odgovora na prijetnju smislena i jednostavna za primjenu. Tačnije, pozitivna predviđanja o efikasnosti odgovora na prijetnju i samoefikasnosti dovešće do veće motivacije za zaštitu, dok će veći troškovi odgovora dovesti do niže motivacije za zaštitu (Sommestad *et al*., 2015).

PMT proučava psihološke i sociološke faktore koji utiču na motivaciju zaposlenih da štite informacije, te traži odgovore na pitanja kao što su:

1. Kako motivisati zaposlene da preuzmu odgovornost za zaštitu informacija i sistema?
2. Kako povećati svijest zaposlenih o važnosti zaštite informacija?
3. Kako poboljšati prihvatanje politika i praksi zaštite informacija od strane zaposlenih?

U međuvremenu, *PMT* je mijenjana i prilagođavana različitim istraživačkim područjima, iako se primarno odnosila na zdravstveni sektor i psihološka istraživanja u pogledu toga kako motivisati ljude da više brinu o svom zdravlju (uticaj straha na motivaciju za brigu o zdravlju).

PMT pruža temeljno znanje o tome zašto ljudi možda ne koriste preporučena odbrambena ponašanja kao odgovor na rizike u oblasti informacione sigurnosti (Herath i Rao, 2009).

PMT uzima u obzir strah (osjećaj koji se javlja kao reakcija na opasnost) kao jedan od centralnih konstrukata koji se posebno istražuje, a pri čemu se ističe da veći strah od prijetnje informacionoj sigurnosti rezultira većom motivacijom za zaštitu, što posljedično rezultira sprovođenjem zaštitnog ponašanja pojedinca (Patel, 2021).

Strah kao pojedinačni konstrukt utiče na motivaciju za zaštitu, a na njega utiču druga dva faktora - percepcija ozbiljnosti prijetnje i percepcija ranjivosti pojedinca. Naime, Boss *et al*. (2015) u svom istraživanju pokazuju da što je veća ozbiljnost prijetnje i percepcija ranjivosti pojedinca, to je veća vjerovatnoća da će on imati strah i biti motivisan da se zaštiti, te pokazati zaštitno ponašanje. Pri tome, treba istaći da percepcija ozbiljnosti prijetnje i percepcija ranjivosti imaju dvostruko dejstvo – utiču direktno na motivaciju za zaštitu, ali i indirektno (posredstvom straha). U baznom PMT modelu izostavlja se strah kao konstrukt, jer ima ulogu posrednika, dok se u proširenom modelu on zadržava (Boss *et al*., 2015).

PMT u proširenom obliku uvodi i konstrukt obuke zaposlenih (eng. *Security Education Training Awareness, SETA*), a koji ima direktan uticaj na zaštitno ponašanje zaposlenika (Posey *et al*., 2015). Naime, autori u svom istraživanju pokazuju da što je obuka zaposlenika kvalitetnija, to je veća vjerovatnoća da će zaposlenici preduzeti adekvatna zaštitna ponašanja kako bi izbjegli sigurnosne prijetnje.

SETA programi, kako je vidljivo iz naziva, sastoje se od tri osnovna elementa: edukacije, treninga i jačanja svijesti zaposlenika. Ipak, budući da organizacije možda nisu u mogućnosti ili ne žele da se nosi sa sva tri navedena zadatka, neke od njih bi mogla prepustiti eksternim saradnicima ili obrazovnim institucijama (Whitman i Mattord, 2022).

Programi obuke pružaju strukturu za planiranje odgovora na prijetnje, edukuju zaposlene o bezbjednosnim problemima sa kojima se njihova kompanija suočava, njihovoj ulozi u odbrani od tih prijetnji i razlozima zbog kojih su te prijetnje usmjerene na njihovu kompaniju (Posey *et al*., 2015).

Svrha *SETA*-e je da poboljša informacionu sigurnost osiguravajući (Whitman i Mattord, 2022):

1. Jačanje svijesti zaposlenih o potrebi zaštite informacionih resursa;
2. Razvoj vještina i znanja kako bi korisnici računara mogli sigurnije obavljati svoje poslove (zaposlenima se pružaju detaljne informacije i praktična uputstva);
3. Stvaranje dubinskog znanja o dizajniranju, implementaciji ili upravljanju sigurnosnim programima za organizacije i sisteme.

Sve navedene aktivnosti doprinose smanjenju rizika od uspješnih napada na informacionu infrastrukturu i osiguravaju da zaposlenici imaju prave alate i znanja za borbu protiv sigurnosnih prijetnji. Neki od primjera su: obuka o pravilima i procedurama sigurnog korištenja računara, zaštiti lozinki, prepoznavanju *phishing* poruka, informisanje o novonastalim prijetnjama i slično.

Od navedena tri elementa *SETA* programa, najmanje se koristi jačanje svijesti korisnika, iako je najjeftinije, te može uključivati jednostavne tehnike, kao što su dijeljenje biltena, postera, video zapisa i drugih sitnica koji podsjećaju zaposlene na važnost informacione sigurnosti (Whitman i Mattord, 2022). Autori navode da su od navedenih tehnika, bilteni (eng. *newsletter*) najisplativija metoda širenja sigurnosnih informacija (mogu se distribuirati u papirnom ili digitalnom obliku), te mogu pomoći da se ideja o sigurnosti informacija zadrži u pamćenju korisnika.

Takođe, autori navode da svi zaposleni u organizaciji obavezno moraju biti obučeni i upoznati sa sigurnošću informacija, ali se podrazumijeva da nije svakom članu organizacije potrebna formalna diploma ili certifikat iz oblasti informacione sigurnosti. Takođe, i Grassegger i Nedbal (2021) u svom istraživanju pobijaju hipotezu da *SETA* programi nemaju statistički značajan uticaj na svjesnost pojedinca o informacionoj sigurnosti. Dakle, zanemarivanje sigurnosnih pitanja zbog nedostatka programa podizanja svijesti može značajno povećati rizik od sigurnosnih prijetnji.

3. METODOLOGIJA I REZULTATI EMPIRIJSKOG ISTRAŽIVANJA

3.1. Metodologija empirijskog istraživanja

3.1.1. Strukturalno modeliranje jednačina (SEM)

Strukturalno modeliranje jednačina (eng. *Structural Equation Modeling, SEM*) je metoda multivarijantne analize koja se primjenjuje za analizu složenih zavisnih veza između različitih varijabli i latentnih konstrukata, ali i između više latentnih konstrukata (Hair *et al*., 2010). Drugi naziv joj je analiza latentnih varijabli (Bajgorić *et al*., 2019).

SEM metodu je razvio švedski naučnik i profesor statistike na Univerzitetu Uppsala u Švedskoj, Karl Jöreskog (Mateos-Aparicio, 2011). Prije pojave SEM metode, 1977. godine nastala je PLS metoda (metoda djelimičnih najmanjih kvadrata), koja je bila rezultat dugogodišnjeg rada švedskog profesora Hermana Wolda (mentora Karla Jöreskog) koji je bio prvi profesor statistike na Univerzitetu Uppsala (Mateos-Aparicio, 2011). Nastala je kao rezultat potrebe da se ublaži problem multikolinearnosti u tradicionalnim regresionim modelima (visoke korelacije između dvije ili više varijabli koja otežava razdvajanje pojedinačnih doprinosa svake varijable u modelu i smanjuje pouzdanost rezultata testiranja hipoteza).

Model koji nastaje upotrebom SEM-a je pojednostavljena slika teorijskih postulata. Za potrebe pravljenja modela, ključnu ulogu u SEM metodi imaju jednačine – one se koriste za opisivanje i modelovanje odnosa između varijabli, čime omogućavaju i suštinsko testiranje teorijskih pretpostavki. Drugim riječima, SEM analizira veze između varijabli koje su strukturno izražene u vidu niza jednačina koje opisuju kako varijable međusobno utiču jedna na drugu, a sve u sklopu datog teorijskog okvira.

Važna prednost korištenja SEM metode je poboljšanje pouzdanosti statističkih procjena, odnosno smanjenje greški mjerenja (koje su neminovno prisutne) zahvaljujući korištenju skupa više različitih varijabli (indikatora) za objašnjenje pojedinog koncepta (Knoke, 2005).

Konstrukti su skriveni ili nevidljivi (latentni) faktori koji se sastoje od više varijabli (zavisnih i nezavisnih) (Hair *et al*., 2010). Manifestne varijable su one koje se mogu direktno kvantifikovati i izmjeriti, dok se latentne varijable (hipotetički/apstraktni koncepti) ne mogu direktno opaziti niti kvantifikovati, već se mjere indirektno na osnovu analize više manifestnih varijabli (indikatora) (Hair *et al*., 2010). Podaci o indikatorima se prethodno prikupljaju različitim metodama (npr. anketom, koja je odabrana i u ovom radu). Dakle, manifestna varijabla je isto što i indikator, a koristi se kako bi se mjerio latentni konstrukt (Bajgorić *et al*, 2019).

SEM kombinuje elemente faktorske analize i višestruke regresije, ali ide i korak dalje, jer osim što omogućava modeliranje odnosa između opaženih (manifestnih) varijabli (slično višestrukoj regresiji), SEM omogućava i modeliranje latentnih konstrukata (slično faktorskoj analizi), a uz sve to i uočavanje uzročno-posljedičnih veza između varijabli (Hair *et al*., 2010).

SEM je specifičan po tome što se svi odnosi između varijabli procjenjuju istovremeno (simultano), tj. odnosi između varijabli ne izučavaju se pojedinačno, kakva je praksa kod modela višestruke regresije. Dakle, SEM cjelovito posmatra sve veze između datih konstrukata (uključujući i zavisne i nezavisne varijable) (Hair *et al*., 2010).

U ovom master radu, SEM metoda je omogućila da se identifikuju uzročno-posljedične veze između faktora koji utiču na zaštitno ponašanje pojedinaca od napada socijalnim inženjeringom.

Izabrani softver za analizu podataka i testiranje hipoteza bio je SmartPLS 4 koji primjenjuje PLS-SEM metodu (eng. *Partial Least Square – Structural Equation Modeling*), a koji je često korišten u istraživačkim radovima zahvaljujući mogućnosti generisanja i analize složenih strukturalnih modela.

3.1.2. Proces prikupljanja podataka

Nakon završenog sekundarnog istraživanja koje je iznjedrilo teorijsku osnovu master rada, pristupljeno je primarnom prikupljanja podataka. Primarno prikupljanje podataka podrazumijevalo je dizajn i sprovođenje online ankete u cilju dolaženja do što većeg broja odgovora od ispitanika na postavljena pitanja, kako bi se osigurala relevantnost dobijenih rezultata, odnosno kako bi se dobila reprezentativna slika percepcije i ponašanja posmatrane populacije.

Anketa je kreirana pomoću online alata za ankete pod nazivom LimeSurvey, u okviru kojeg je izvršeno i šifriranje svih pojedinih pitanja, što je bilo važno za kasniju analizu. Otvorena

je za popunjavanje 15.8.2023. godine, a zatvorena 8.9.2023. godine kada je dostignuta cifra od ukupno 234 ispitanika (od čega su 223 ispitnika prošla filter pitanja kojima je osigurano da su ispitivani isključivo stanovnici Bosne i Hercegovine koji su zaposleni).

Važno je napomenuti i da je u postavkama ankete izabrano podešavanje da svi odgovori u anketi budu anonimni kako bi se obezbijedila privatnost ispitanika. Takođe, napomenom da je anketa anonimna nastojalo se podstaći ispitanike da se osjećaju slobodno da daju iskrene odgovore na postavljena pitanja, odnosno da bezrazložno ne teže davanju društveno prihvatljivih odgovora u želji da se prilagode očekivanjima ispitivača. LimeSurvey je izabran primarno zbog svoje jednostavnosti, ali i efikasnosti prikupljanja podataka od ispitanika, budući da su ispitanici na pitanja u anketi odgovarali pomoću svojih pametnih telefona/tableta ili računara, odnosno anketa im je bila lako dostupna. Takođe, zabilježeni odgovori su sigurno pohranjeni u LimeSurvey bazu podataka koja je kasnije korištena za uvoz podataka u softver za analizu koji je odabran (SmartPLS 4).

Anketa je distribuirana putem interneta, primarno putem društvenih mreža (Facebook, Linkedin), zatim putem aplikacija za instant komunikaciju, ali i direktnim slanjem e-mail poruka sa molbom za popunjavanje ankete. Određeni problem i faktor usporavanja procesa prikupljanja odgovora predstavljala je situacija da su pojedini ispitanici napuštali popunjavanje ankete prije njenog završetka tako da su njihovi odgovori bili nepotpuni, a što je onemogućilo uzimanje u obzir njihovih odgovoru u finalnim i zbirnim rezultatima ankete. Dakle, u obziru su uzeti samo odgovori ispitanika koji su anketu popunili u cjelini od početka od kraja. Takođe, aktivna distribucija ankete je vršena u više odvojenih navrata, uvijek različitim pojedincima, sve dok nije postignut zadovoljavajući broj ispitanika.

3.1.3. Opis uzorka

Ispitanici ankete su bili pojedinci stariji od 18 godina, koji su zaposleni i žive u Bosni i Hercegovini. Prva dva pitanja u anketi, „Da li živite na teritoriji Bosne i Hercegovine?“ i „Da li ste trenutno zaposleni?“, služila su kao filter, tako da ako je odgovor bio ne na bilo koje pitanje, anketa se završavala za tog ispitanika. Na taj način, iako je bilo ukupno 234 potpuna odgovora, 11 ispitanika nije nastavljalo anketu jer su bili nezaposleni ili nisu živjeli u Bosni i Hercegovini.

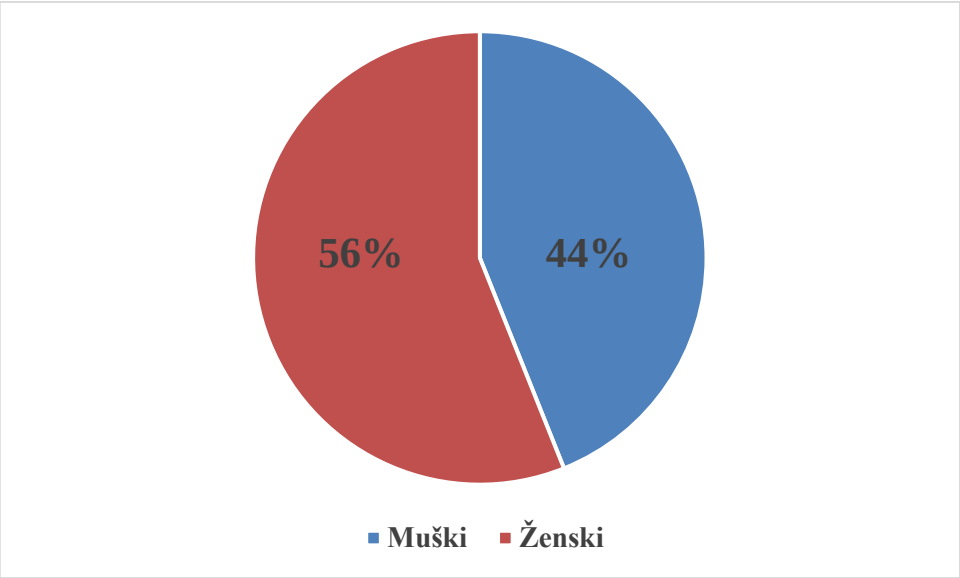
Polna struktura ispitanika pokazuje da je ženskih ispitanika bilo blago više (56,05%), a opšta raspodjela polova ispitanika vidljiva je u tabeli 1. i grafikonu 1.

Tabela 1. Polna struktura ispitanika

Odgovor	Ukupno	Postotak
Muški	98	43,95%
Ženski	125	56,05%
Ukupno	**223**	**100%**

Izvor: Izrada autora

Grafikon 1. Polna struktura ispitanika



Izvor: Izrada autora

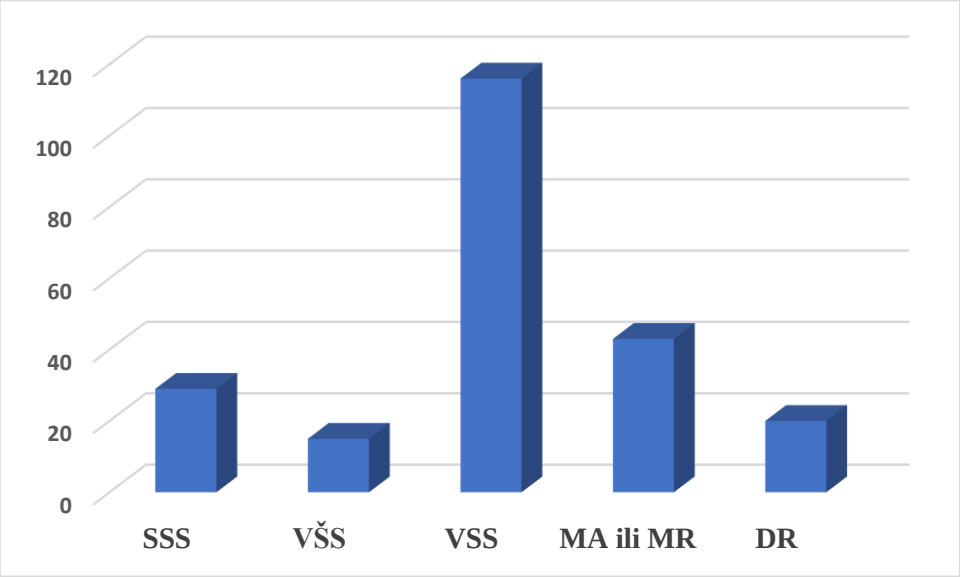
Nivo obrazovanja većine ispitanika (52,02%) je visoka stručna sprema (VSS), a zatim slijede ispitanici sa završenim master studijama (19,28%), te srednjom stručnom spremom (13%), što je vidljivo u tabeli 2. i grafikonu 2.

Tabela 2. Obrazovna struktura ispitanika

Odgovor	Ukupno	Postotak
SSS	29	13,00%
VŠS	15	6,73%
VSS	116	52,02%
MA ili MR	43	19,28%
DR	20	8,97%
Ukupno	**223**	**100%**

Izvor: Izrada autora

Grafikon 2. Obrazovna struktura ispitanika



Izvor: Izrada autora

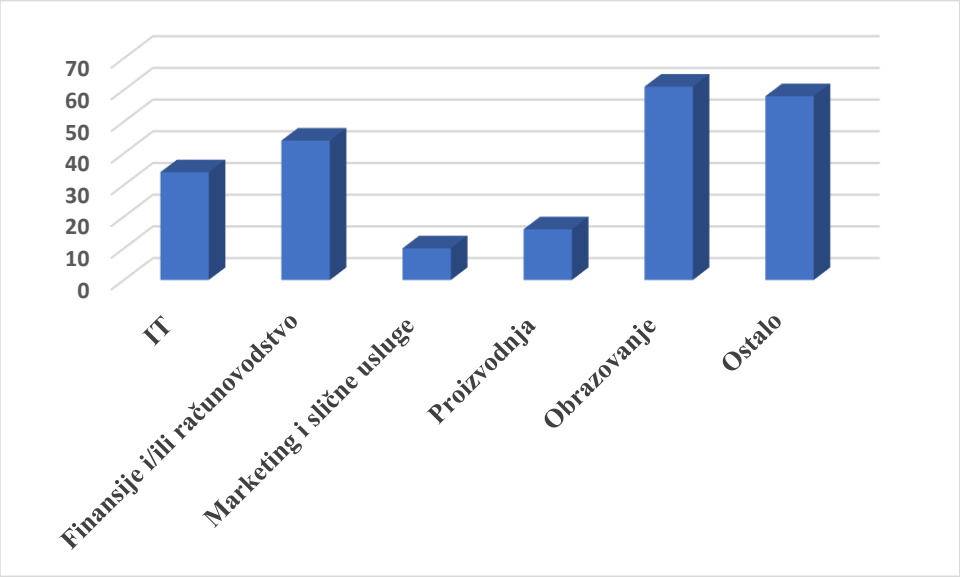
Tabela 3. i grafikon 3. prikazuju u kojoj industriji su zaposleni ispitanici. Od ponuđenih, tri industrije su se istakle kao dominantne među ispitanicima, a to su obrazovanje i finansije i/ili računovodstvo, a zatim i IT sektor (u ove tri industrije ubrojano je 62,33% ispitanika). Kategorija "Ostalo" takođe je imala značajan udio (26,01%).

Tabela 3. Industrija u kojoj su zaposleni ispitanici

Odgovor	Ukupno	Postotak
IT	34	15,25%
Finansije i/ili računovodstvo	44	19,73%
Marketing i slične usluge	10	4,48%
Proizvodnja	16	7,17%
Obrazovanje	61	27,35%
Ostalo	58	26,01%
Ukupno	**223**	**100%**

Izvor: Izrada autora

Grafikon 3. Industrija u kojoj su zaposleni ispitanici



Izvor: Izrada autora

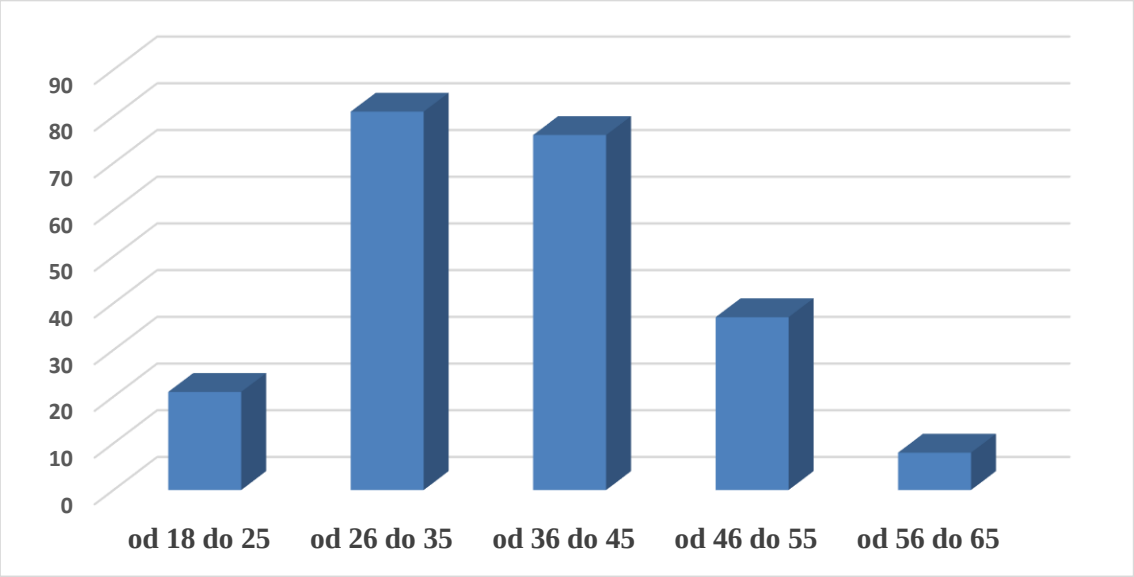
Starosna struktura ispitanika prikazana je u tabeli 4. i grafikonu 4., a iz nje je vidljivo da je najveći broj ispitanika imao od 26 do 35 (36,32%), te 36 do 45 godina (34,08%), što je zbirno gledajući 70,40% ispitanika.

Tabela 4. Starosna struktura ispitanika

Odgovor	Ukupno	Postotak
od 18 do 25	21	9,42%
od 26 do 35	81	36,32%
od 36 do 45	76	34,08%
od 46 do 55	37	16,59%
od 56 do 65	8	3,59%
Ukupno	**223**	**100%**

Izvor: Izrada autora

Grafikon 4. Starosna struktura ispitanika



Izvor: Izrada autora

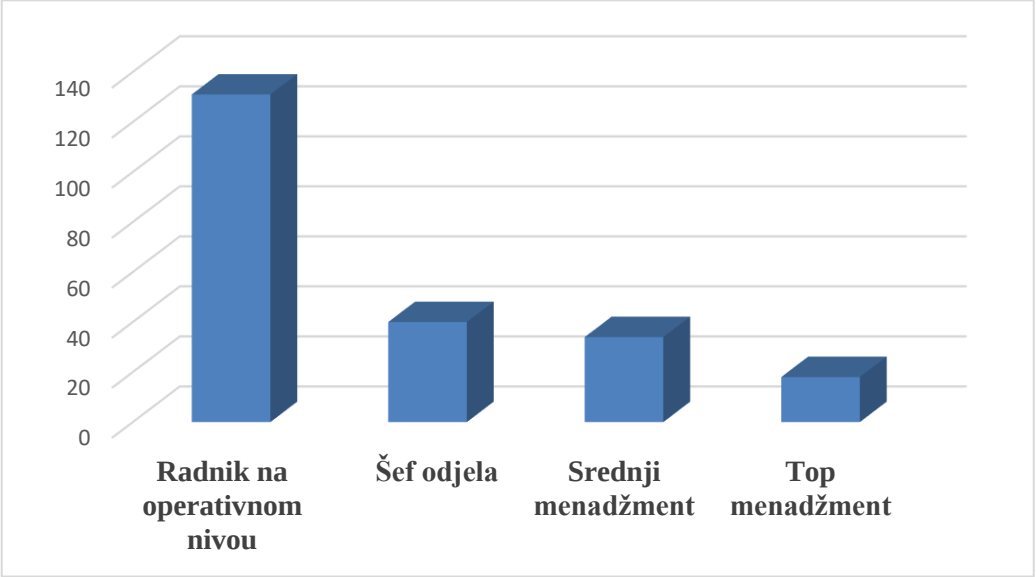
Tabela 5. i grafikon 5. prikazuju hijerarhijske pozicije ispitanika u njihovim kompanijama. Vidljivo je da ih većina obavlja rad na operativnom nivou (58,74%), što odražava uobičajenu hijerarhijsku strukturu organizacija, gdje se na operativnom nivou uvijek nalazi najveći broj zaposlenika koji obavljaju svakodnevne zadatke neophodne za funkcionisanje organizacije.

Tabela 5. Hijerarhijska pozicija ispitanika u kompanijama

Odgovor	Ukupno	Postotak
Radnik na operativnom nivou	131	58,74%
Šef odjela	40	17,94%
Srednji menadžment	34	15,25%
Top menadžment	18	8,07%
Ukupno	**223**	**100%**

Izvor: Izrada autora

Grafikon 5. Hijerarhijska pozicija ispitanika u kompanijama



Izvor: Izrada autora

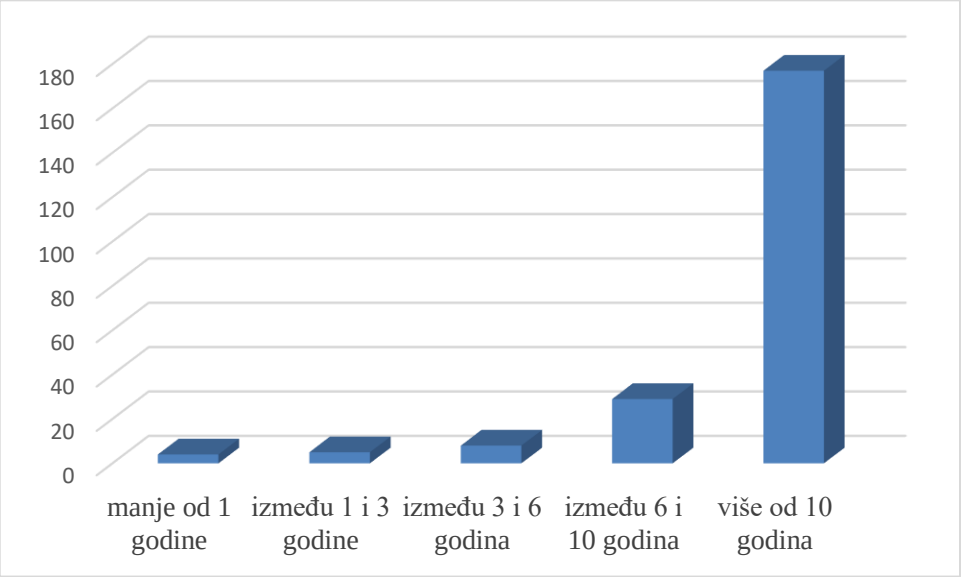
Tabela 6. i grafikon 6. pokazuju koliko iskustva ispitanici imaju u korištenju računara, gdje je vidljivo da ih velika većina (79,37%) ima dugogodišnje iskustvo u poznavanju digitalnih tehnologija (više od 10 godina).

Tabela 6. Iskustvo ispitanika u korištenju računara (u godinama)

Odgovor	Ukupno	Postotak
manje od 1 godine	4	1,79%
između 1 i 3 godine	5	2,24%
između 3 i 6 godina	8	3,59%
između 6 i 10 godina	29	13,00%
više od 10 godina	177	79,37%
Ukupno	**223**	**100%**

Izvor: Izrada autora

Grafikon 6. Iskustvo ispitanika u korištenju računara (u godinama)



Izvor: Izrada autora

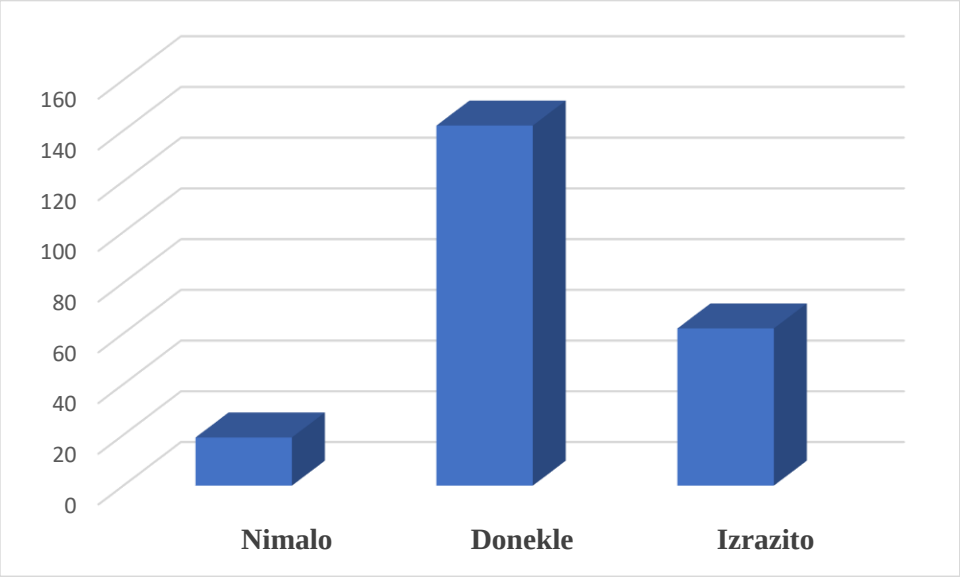
Najzad, tabela 7. i grafikon 7. pokazuju procjenu ispitanika o njihovoj dosadašnjoj izloženosti napadima socijalnim inženjeringom (postavljeno pitanje je glasilo: „Koliko ste do sad bili izloženi računarskim napadima socijalnim inženjeringom (npr. da ste dobili lažnu poruku ili e-poštu kojima je neko pokušao da Vas prevari tako što se lažno predstavio i zatražio od Vas neke lične informacije)?“. Zbirno gledajući, 91,48% ispitanika je bilo bar nekad (donekle) ili često (izrazito) izloženo napadima socijalnim inženjeringom, što ukazuje da je socijalni inženjering učestala prijetnja njihovoj informacionoj sigurnosti.

Tabela 7. Dosadašnja izloženost ispitanika napadima socijalnim inženjeringom

Odgovor	**Ukupno**	**Postotak**
Nimalo	19	8,52%
Donekle	142	63,68%
Izrazito	62	27,80%
Ukupno	**223**	**100%**

Izvor: Izrada autora

Grafikon 7. Dosadašnja izloženost ispitanika napadima socijalnim inženjeringom



Izvor: Izrada autora

3.2. Rezultati i interpretacija rezultata empirijskog istraživanja

Sirovi podaci prikupljeni anketom uvezeni su u SmartPLS 4 softver kako bi se ispitala međusobna povezanost konstrukata i testirale postavljene hipoteze.

Za uočavanje korelacije između postavljenih konstrukata korišten je „*consistent PLS-SEM algoritam*“, a u cilju testiranja hipoteza i „*consistent PLS-SEM bootstraping*“ kao statistička procedura u kojoj su sve varijable reflektivne, a ne formativne, čime se težilo da se izbjegnu potencijalne greške u interpretaciji rezultata. Naime, korištene reflektivne varijable su zapravo indikatori pojedinog latentnog konstrukta (koji se ne mjeri direktno, već procjenjuje na osnovu saznanja o više reflektivnih varijabli koje ga čine).

Izračunati koeficijenti putanja (eng. *path coefficients*) kroz „*consistent PLS-SEM algoritam*“ predstavljeni su u tabeli 8.

Tabela 8. Koeficijenti putanja

	Koeficijenti putanja
Percipirana ozbiljnost -> Strah	0,400
Percipirana ranjivost -> Strah	0,515
Strah -> Motivacija za zaštitu	0,217
Percipirana ozbiljnost -> Motivacija za zaštitu	0,404
Percipirana ranjivost -> Motivacija za zaštitu	0,017
Motivacija za zaštitu -> Zaštitno ponašanje	0,467
Obuka zaposlenih -> Zaštitno ponašanje	0,202

Izvor: Izrada autora

Dobijeni koeficijenti putanje tumačeni su nakon uzimanja u obzir rezultata dobijenih sprovođenjem „*consistent PLS-SEM bootstrapping*-a“ koji je pokazao vrijednosti t-statistike i p-vrijednost.

Da bi se hipoteza testirala sproveden je t-test za nivo značajnosti od 5% ($\alpha = 0,05$). Pri tome, da bi se određena hipoteza prihvatila potrebno da vrijednost dvosmjernog t-testa bude izvan raspona od ±1,96 (Hair *et al*., 2017). Naime, vrijednost 1,96 odgovara kritičnom pragu za nivo značajnosti od 5% u dvosmjernom t-testu jer je 95% površine t-distribucije smješteno unutar intervala ±1,96. Ako je t-vrijednost unutar ovog intervala, to znači da nema statistički značajnih odstupanja. S druge strane, ako t-vrijednost izlazi izvan navedenog intervala, to ukazuje na statističku značajnost rezultata (Hair *et al*., 2017).

Nivo značajnosti od 5% podrazumijeva da prihvatamo rizik od 5% da će se desiti greška tipa 1 (pogrešno odbacivanje hipoteze koja je zapravo tačna). Dakle, ako ustanovimo da je vrijednost t-testa 1, 96 ili veća, to znači da je vjerovatnoća da smo pogriješili manja ili jednaka 5%.

Nadalje, da bi hipoteza bila podržana, potrebno je da p-vrijednost bude manja ili jednaka 0,05 (Hair *et al*., 2017).

Na temelju modela izrađenog u SmartPLS-u dobijeni su kvantitativni pokazatelji, t-statistika i p-vrijednost, koji su predstavljeni u tabeli 9.

Tabela 9. T-statistika i p-vrijednost

	Originalni uzorak (O)	Srednja vrijednost uzorka (M)	St. devijacija (STDEV)	**T statistika (|O/STDEV|)**	**P vrijednost**
PO -> ST	0,400	0,401	0,069	5,805	0,000
PR -> ST	0,515	0,516	0,069	7,443	0,000
ST -> MZ	0,217	0,212	0,126	1,716	0,086
PO -> MZ	0,404	0,407	0,110	3,665	0,000
PR -> MZ	0,017	0,018	0,113	0,155	0,877
MZ -> ZP	0,467	0,473	0,085	5,517	0,000
OZ -> ZP	0,202	0,209	0,084	2,416	0,016

Izvor: Izrada autora

Iz tabele je vidljivo da je t-statistika za pet hipoteza (od njih ukupno sedam) zadovoljila postavljeni uslov (veća je od 1,96), te da je za tih pet hipoteza i p-vrijednost zadovoljila postavljeni uslov (manja je od 0,05). Za preostale dvije hipoteze t-statistika manja je od 1,96, a p-vrijednost veća od 0,05.

U tabeli 10. predstavljeni su rezultati testiranja hipoteza iz kojih je vidljivo koje hipoteze se mogu prihvatiti, a za koje nema dovoljno dokaza da se prihvate.

Tabela 10. Sažetak rezultata testiranja hipoteza

Hipoteza	**Rezultat**
H1: **Percipirana ozbiljnost** potencijalnih gubitaka usljed napada socijalnim inženjeringom je pozitivno korelisana sa **strahom** korisnika od napada socijalnim inženjeringom.	Potvrđena
H2: **Percipirana ranjivost** korisnika je pozitivno korelisana sa **strahom** korisnika od napada socijalnim inženjeringom.	Potvrđena
H3: **Strah** korisnika od napada socijalnim inženjeringom je pozitivno korelisan sa **motivacijom** korisnika za zaštitu od napada.	Nije potvrđena
H4: **Percipirana ozbiljnost** potencijalnih gubitaka usljed napada socijalnim inženjeringom je pozitivno korelisana sa **motivacijom** korisnika za zaštitu od napada.	Potvrđena
H5: **Percipirana ranjivost** korisnika je pozitivno korelisana sa **motivacijom** korisnika za zaštitu od napada.	Nije potvrđena
H6: **Motivacija** korisnika za zaštitu od napada je pozitivno korelisana sa **zaštitnim ponašanjem**.	Potvrđena
H7: Sprovođenje **obuke** zaposlenih o sigurnosnim procedurama je pozitivno korelisano sa **zaštitnim ponašanjem**.	Potvrđena

Izvor: Izrada autora

Potvrđene hipoteze ukazuju na statistički značajnu pozitivnu povezanost između percepcije sigurnosnih aspekata i korisničkog ponašanja u kontekstu socijalnog inženjeringa.

Konkretno, rezultati potvrđuju da percepcija ozbiljnosti mogućih gubitaka i ranjivosti korisnika pozitivno utiču na strah korisnika od napada socijalnim inženjeringom (H1 i H2). Takođe je utvrđeno da percipirana ozbiljnost potencijalnih gubitaka ima statistički značajnu ulogu u motivaciji korisnika za zaštitu od napada socijalnim inženjeringom (H4).

Osim toga, motivacija korisnika za zaštitu od napada socijalnim inženjeringom pokazala se kao statistički značajan faktor koji pozitivno utiče na zaštitno ponašanje ispitanika (H6). Nadalje, potvrđeno je da sprovođenje obuke zaposlenih o sigurnosnim procedurama ima statistički značajan pozitivan uticaj na njihovo zaštitno ponašanje (H7).

S druge strane, hipoteze H3 i H5 nisu prihvaćene jer analiza podataka nije otkrila statistički značajne korelacije između straha korisnika od napada socijalnim inženjeringom i njihove motivacije za zaštitu od napada, niti između percipirane ranjivosti korisnika i njihove motivacije za zaštitu. Razlog bi mogao biti u tome što su anketirani ispitanici izloženi različitim faktorima koji takođe utiču na njihovu percepciju i motivaciju, a koji nisu obuhvaćeni u okviru ovog istraživanja. Iako nisu pronađene statistički značajne korelacije u ovom konkretnom kontekstu, to nužno ne ukazuje na potpuni izostanak veze između navedenih varijabli. Dakle, važno je naglasiti da kod hipoteza H3 i H5 podaci ukazuju na pozitivnu korelaciju, ali taj odnos nije statistički značajan. Moguće je da postoji složenija dinamika odnosa između percepcije ranjivosti, straha od napada i motivacije za zaštitu, uključujući i mogućnost da korisnici sa nižom percepcijom ranjivosti možda nemaju strah od napada i stoga posljedično nemaju ni jaku motivaciju za zaštitu od njih.

Važan pokazatelj koji je takođe uzet u razmatranje je koeficijent determinacije (R^2). Koeficijent determinacije pokazuje koji postotak varijabilnosti zavisne varijable može biti objašnjen uključivanjem odabranih nezavisnih varijabli u model. R^2 se interpretira kao omjer između objašnjene varijabilnosti i ukupne varijabilnosti, a njegova vrijednost kreće se u rasponu od 0 do 1 (Somun-Kapetanović, 2012). Što je viša vrijednost R^2 to znači da je model uspješniji u objašnjavanju varijabilnosti zavisne varijable.

Tabela 11. pokazuje dobijene vrijednosti koeficijenta determinacije i prilagođenog koeficijenta determinacije za predstavljeni model.

Tabela 11. Koeficijent determinacije

	R^2	**R^2** prilagođeno
Strah	0,643	0,639
Motivacija za zaštitu	0,341	0,332
Zaštitno ponašanje	0,320	0,314

Izvor: Izrada autora

Dobijene vrijednosti koeficijenta determinacije (kao i prilagođenog koeficijenta determinacije) mogu se smatrati zadovoljavajućim s obzirom da je riječ o kompleksnim i

latentnim konstruktima. Naime, istraženi konstrukti su po svojoj suštini određeni subjektivnim iskustvom ispitanika, te je očekivano da ostaje dio neobjašnjenog varijabiliteta motivacije za zaštitu, straha i zaštitnog ponašanja usljed postojanja faktora koji nisu obuhvaćeni predstavljenim modelom.

Takođe, u tabeli 12. prikazane su vrijednosti F^2 pokazatelja koji pokazuje koliko su egzogeni (nezavisni) konstrukti doprinijeli koeficijentu determinacije endogenih (zavisnih) konstrukata (koji su predstavljeni modelom) (Hair *et al*., 2017).

Tabela 12. Vrijednost F^2

	F^2
Percipirana ozbiljnost -> Strah	0,324
Percipirana ranjivost -> Strah	0,536
Strah -> Motivacija za zaštitu	0,026
Percipirana ozbiljnost -> Motivacija za zaštitu	0,135
Percipirana ranjivost -> Motivacija za zaštitu	0,000
Motivacija za zaštitu -> Zaštitno ponašanje	0,286
Obuka zaposlenih -> Zaštitno ponašanje	0,054

Izvor: Izrada autora

Vidljivo je da je vrijednost F^2 izrazito niska (F^2 = 0,000) u odnosu percipirane ranjivosti i motivacije za zaštitu što takođe ukazuje (kao i kod koeficijenta determinacije) da varijacija u motivaciji za zaštitu nije znatno objašnjena prisutnošću ili doprinosom percipirane ranjivosti, te da postoji značajna neobjašnjena varijabilnost u motivaciji za zaštitu koju ovaj model nije uspio predstaviti. Isti je slučaj i sa odnosom straha i motivacije za zaštitu (F^2 = 0,026), tj. i u ovom slučaju je vidljivo da strah nema značajan doprinos u objašnjavanju varijabilnosti motivacije za zaštitu.

Najzad, u tabeli 13. prikazuje se vrijednost Q^2. Ako je Q^2 veće od nula, to znači da je predstavljeni model relevantan za predviđanja (Hair *et al*., 2017), a navedeni uslov zadovoljen je za sva tri posmatrana zavisna konstrukta.

Tabela 13. Vrijednost Q^2

	Q^2
Strah	0,555
Motivacija za zaštitu	0,251
Zaštitno ponašanje	0,109

Izvor: Izrada autora

3.3. Ograničenja sprovedenog istraživanja

Potencijalno ograničenje sprovedenog istraživanja ogleda se u tome što ono uzima u obzir subjektivne stavove i mišljenja ispitanika o socijalnim inženjeringu. Odnosno, anketa ne simulira stvarni strah i stres koji bi ispitanici doživjeli da zaista postanu žrtva sajber napada i izgube dragocjene podatke, reputaciju ili neko zloupotrijebi njihov identitet. Takođe, u situaciji kada su informaciono bezbjedni, odnosno nisu trenutno izloženi riziku (tj. tokom samog popunjavanja ankete), ispitanici mogu da precijene svoja znanja i vještine koje posjeduju za odbranu od socijalnog inženjeringa. S druge strane, ispitanici mogu i da potcijene ozbiljnost posljedica takvog incidenta u svom poslovnom ili privatnom životu. Dakle, iako ispitanici mogu pokušati da zamisle svoju reakciju na saznanje da su prethodno izmanipulisani nekom od taktika socijalnog inženjeringa, to nužno ne odražava kako bi se oni osjećali i postupali kada bi stvarno bili suočeni sa ovim problemom.

Uprkos navedenim ograničenjima, sprovedena anketa se pokazala kao korisna metoda za istraživanje subjektivnih stavova i mišljenja, te planiranih postupaka ispitanika u vezi sa odbranom od prijetnje po informacionu sigurnost u vidu socijalnog inženjeringa.

4. ZAKLJUČAK

Prva četiri istraživačka cilja, koja su obuhvatala elaboraciju osnovnih teorijskih postulata u vezi sa socijalnim inženjeringom kao potencijalnom prijetnjom za sigurnost informacionih sistema, kao i analizu različitih vrsta, faza i načina odbrane od napada, ostvarena su putem prezentacije rezultata sekundarnog istraživanja, što je detaljno predstavljeno u teorijskom okviru ovog rada (drugo poglavlje).

Sekundarno istraživanje pokazalo je da je socijalni inženjering jedna od najznačajnijih prijetnji za sigurnost informacionih sistema. Razlog njegove uspješnost je u tome što iskorištava najranjiviju tačku svakog informacionog sistema – ljude koji ga koriste i njime upravljaju. Korištenjem različitih metoda, kao što su manipulisanje, lažno predstavljanje, stvaranje osjećaja hitnosti ili privida prijateljstva i odnosa od povjerenja sa žrtvom, napadači dolaze do željenih podataka.

Lozinke, korisnička imena, podaci o kupcima, konkurentima ili poslovnim tajnama određene kompanije dolaskom u ruke napadača predstavljaju izvor finansijske ili nefinansijske koristi za napadača, što ih motiviše da koriste socijalni inženjering kao metodu napada.

Postoji mnogo različitih vrsta socijalnog inženjeringa (od kojih je najpoznatija *phishing*), ali sve slijede slične faze realizacije. To su prikupljanje podataka o žrtvi, razvijanje veze sa njom, eksploatacija njenog znanja i na kraju prekid kontakta. Da bi se izbjegle štete i gubici koji nastaju usljed prodora socijalnim inženjeringom, potrebno je uspostaviti i koristiti mehanizme odbrane kao što je edukacija u okviru višeslojne odbrane od napada. Posebno se izdvaja važnost preventivne, proaktivne i reaktivne odbrane. Preventivna odbrana se

fokusira na sprečavanje napada prije nego što se dogodi, proaktivna odbrana usmjerena je na rano otkrivanje i reagovanje prije nego što napad izmakne kontroli, dok se reaktivna odbrana bavi suzbijanjem i saniranjem posljedica nakon što se napad dogodi.

Kao temeljni teoretski okvir i jezgro za empirijsko istraživanje u okviru ovog master rada poslužila je teorija motivacije za zaštitu (PMT), koja pojašnjava šta motiviše ljude da štite informacije i sisteme u organizacijama u kojima rade.

Peti istraživački cilj, koji se odnosio na analizu percepcije i zaštitno ponašanje korisnika informacionih tehnologija u Bosni i Hercegovini prema prijetnjama od napada socijalnim inženjeringom na informacionu sigurnost, zadovoljen je kroz detaljnu ekspoziciju metodologije i prezentaciju rezultata empirijskog istraživanja (treće poglavlje).

Empirijski pristup istraživanju bio je kvantitativni, a sastojao se od prikupljanja podataka, analize podataka, te interpretacije rezultata i donošenja zaključka. Primarna kvantitativna istraživačka metoda korištena u radu je strukturalno modeliranje jednačina (eng. *Structural Equation Modeling, SEM*). Prikupljanje podataka izvršeno je realizacijom *online* ankete na osnovu koje su prikupljena 223 odgovora pojedinaca koji su zaposleni u Bosni i Hercegovini, a stariji su od 18 godina. Analiza podataka i testiranje postavljenih hipoteza izvršeno je uz pomoć SmartPLS 4 softvera.

Od ukupno sedam postavljenih hipoteza, pet ih je dobilo potvrdu u okviru istraživanja, dok dvije nisu prihvaćene zbog nedostizanja zadovoljavajućeg nivoa statističke značajnosti.

Potvrđene su hipoteze:

- H1: Percipirana ozbiljnost potencijalnih gubitaka usljed napada socijalnim inženjeringom je pozitivno korelisana sa strahom korisnika od napada socijalnim inženjeringom.
- H2: Percipirana ranjivost korisnika je pozitivno korelisana sa strahom korisnika od napada socijalnim inženjeringom.
- H4: Percipirana ozbiljnost potencijalnih gubitaka usljed napada socijalnim inženjeringom je pozitivno korelisana sa motivacijom korisnika za zaštitu od napada.
- H6: Motivacija korisnika za zaštitu od napada je pozitivno korelisana sa zaštitnim ponašanjem.
- H7: Sprovođenje obuke zaposlenih o sigurnosnim procedurama je pozitivno korelisano sa zaštitnim ponašanjem.

Potvrđene hipoteze ukazuju na statistički značajnu povezanost između percepcije sigurnosnih aspekata i korisničkog ponašanja u kontekstu socijalnog inženjeringa. Konkretno, rezultati potvrđuju da percepcija ozbiljnosti mogućih gubitaka i ranjivosti korisnika pozitivno utiču na strah korisnika od napada socijalnim inženjeringom (H1 i H2). Takođe je utvrđeno da percipirana ozbiljnost potencijalnih gubitaka ima statistički značajnu pozitivnu ulogu u motivaciji korisnika za zaštitu od napada socijalnim inženjeringom (H4).

Osim toga, motivacija korisnika za zaštitu od napada socijalnim inženjeringom pokazala se kao statistički značajan faktor koji pozitivno utiče na zaštitno ponašanje ispitanika (H6). Nadalje, potvrđeno je da sprovođenje obuke zaposlenih o sigurnosnim procedurama ima statistički značajan pozitivan uticaj na njihovo zaštitno ponašanje (H7).

Hipoteze koje se ne mogu prihvatiti su:

- H3: Strah korisnika od napada socijalnim inženjeringom je pozitivno korelisana sa motivacijom korisnika za zaštitu od napada.
- H5: Percipirana ranjivost korisnika je pozitivno korelisana sa motivacijom korisnika za zaštitu od napada.

Hipoteze H3 i H5 nisu prihvaćene jer analiza podataka nije otkrila statistički značajne korelacije između straha korisnika od napada socijalnim inženjeringom i njihove motivacije za zaštitu od napada, niti između percipirane ranjivosti korisnika i njihove motivacije za zaštitu. Razlog bi mogao biti u tome što su anketirani ispitanici izloženi različitim faktorima koji takođe utiču na njihovu percepciju i motivaciju, a koji nisu obuhvaćeni u okviru ovog istraživanja. Iako nisu pronađene statistički značajne korelacije u ovom konkretnom kontekstu, to nužno ne ukazuje na potpuni izostanak veze između navedenih varijabli. Moguće je da postoji složenija i suptilnija dinamika između percepcije ranjivosti, straha od napada i motivacije za zaštitu, uključujući i mogućnost da korisnici sa nižom percepcijom ranjivosti možda nemaju strah od napada i stoga posljedično nemaju ni jaku motivaciju za zaštitu od njih. Potencijalno ograničenje sprovedenog empirijskog istraživanja ogleda se u tome što ono uzima u obzir subjektivne stavove i mišljenja ispitanika o socijalnim inženjeringu. Nijedna anketa ne može simulirati stvarni strah i stres koji bi ispitanici doživjeli da zaista postanu žrtva sajber napada i izgube dragocjene podatke, reputaciju ili neko zloupotrijebi njihov identitet, što bi mogao biti i razlog nemogućnosti dokazivanja H3 i H5.

Uprkos navedenim ograničenjima, sprovedeno primarno i sekundarno istraživanje pružili su dublji uvid u kompleksnu prirodu percepcije i ponašanja korisnika u vezi sa napadima socijalnim inženjeringom i sigurnošću informacionih sistema.

Finalni zaključak koji se može iznijeti polazeći od teorijskih postulata i rezultata empirijskog istraživanja u okviru ovog rada podrazumijeva naglašavanje važnosti kontinuirane edukacije i podizanja svijesti kako među korisnicima informacionih sistema, tako i među organizacijama i institucijama odgovornim za njihovu zaštitu. Nijedan informacioni sistem nikada ne može biti apsolutno (stopostotno) siguran, ali je apsolutno sigurno da se brigom isključivo o tehničkim aspektima informacionog sistema neće postići adekvatna zaštita od potencijalnih prijetnji i napada. Važno je u obzir uzeti i ljudski faktor, kao najranjiviju kariku u lancu sigurnosti, a sve u cilju obezbjeđivanja sveobuhvatne zaštite od složenih prijetnji

sigurnosti informacionih sistema, među kojima značajno mjesto zauzima socijalni inženjering.

REFERENCE

1. Abass, I. (2018) Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security*, 9, 257-264.
2. Abawajy, J. (2014). User preference of cyber security awareness delivery methods, *Behaviour & Information Technology, 33:3*, 237-248.
3. Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet, 12*(10), 168.
4. Albladi, S. M. i Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity, 3*(1).
5. Aldawood, H. i Skinner, G. (2018) Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *26th International Conference on Systems Engineering*, Sydney, 1-6.
6. Aldawood, H. i Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet. 11*. 73. 10.3390/fi11030073.
7. Aldawood, H. i Skinner, G. Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access, vol. 8,* 67321-67329. 10.1109/ACCESS.2020.2983280.
8. Alharthi, D. (2021.) Social Engineering Defense Mechanisms and InfoSec Policies: A Survey and Qualitative Analysis. Doctoral dissertation. University of California, Irvine.
9. Allen, M. (2006). Social Engineering: A Means To Violate A Computer System. *Sans Institute.* White Paper.
10. Alsharif, M., Mishra, S. i AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering, 40(3),* 1153–1166.
11. Amazon Web Services. (2023). *Compliance Programs - Amazon Web Services (AWS).*
12. Anti-Phishing Working Group. (2022). *Phishing Activity Trends Report, 3rd Quarter 2022.* APWG.
13. Ashford, W. (2015). *Social engineering attacks more complex than ever, says expert.* ComputerWeekly.com. Dostupno na: https://www.computerweekly.com/news/4500247025/Social-engineering-attacks-more-complex-than-ever-says-expert (Pristupljeno: 3. februara 2023.)
14. Bajgorić, N., Somun-Kapetanović, R., Resić, E. i Turulja, L. (2019). *Uvod u metodologiju naučnoistraživačkog rada.* Drugo izdanje. Sarajevo: Ekonomski fakultet u Sarajevu.
15. Bansla, N., Kunwar, S. i Jain, K. (2019). Social Engineering: A Technique for Managing Human Behavior. *Journal of Information Technology and Sciences, 5 (1),* 18-22.
16. Bhusal, C.S., 2021. Systematic review on social engineering: Hacking by manipulating humans. *Journal of Information Security*, *12*, pp.104-114.
17. Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. i Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864.
18. Breda, F., Barbosa, H. i Morais, T. (2017). Social Engineering and cyber security. *INTED Proceedings*.
19. Civelek, M. E. (2018). *Essentials of structural equation modeling.* Zea Books. Dostupno na: https://doi.org/10.13014/k2sj1hr5 (Pristupljeno: 9. septembra 2023.)
20. Duarte, N., Coelho, N. i Guarda, T. (2021). Social Engineering: The art of attacks. *Communications in Computer and Information Science*, 474–483.

21. Edwards, M., Larson, R., Green, B., Rashid, A. i Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, *69*, 18–34.
22. Fan, W., Lwakatare, K. i Rong, R. (2017). Social Engineering: I-E based model of human weakness for attack and defense investigations. *International Journal of Computer Network and Information Security*, *9*(1), 1–11.
23. Farooq, A., Isoaho, J., Virtanen, S. i Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 352-359.
24. Franchi, E., Poggi, A. i Tomaiuolo, M. (2015). Information and password attacks on social networks. *Journal of Information Technology Research*, *8*(1), 25–42.
25. Google Cloud. (2003). *Google security overview | Documentation.* Dostupno na: https://cloud.google.com/docs/security/overview/whitepaper (Pristupljeno: 18. februara 2023.)
26. Gragg D. (2002). A multi-level Defense Against Social Engineering. *SANS Institute*, San Diego, California, USA. Dostupno na: http://www.sans.org/reading_room/whitepapers/engineering/ (Pristupljeno: 20. februara 2023.)
27. Grassegger, T. i Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science, 181*, 59–66.
28. Grigoryan, L. i Mirzoyan, L. (2023) 'Cybersecurity risks and its regulations. The Philosophy of Cybersecurity Audit', WISDOM, 25(1), pp. 67–77.
29. Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Institute InfoSec Reading Room.*
30. Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. Wiley.
31. Hair, J. F., Hult, G. T. M., Ringle, C. i Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM).* Los Angeles, CA: Sage.
32. Hair, J.F., Black, W. C., Babin, B. J. i Anderson, R. E. (2010). *Multivariate Data Analysis*. 7th edition. New York: Pearson.
33. Harris, M.A. i Martin, R. (2019), 'Promoting cybersecurity compliance', Cybersecurity Education for Awareness and Compliance, pp. 54–71.
34. Hatfield, J. M. (2018). Social engineering in cybersecurity: the evolution of a concept. *Computers & Security, Vol. 73*, 102-113.
35. Heartfield, R. i Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 1–39.
36. Herath, T. i Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.
37. *Imperva Learning Center* (2019). *What is spear phishing: How is it different from whaling attacks:* Dostupno na: https://www.imperva.com/learn/application-security/spear-phishing/ (Pristupljeno: 28. avgusta 2023.)
38. Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E. i Pu, C. (2011). Reverse social engineering attacks in online social networks. *Detection of Intrusions and Malware, and Vulnerability Assessment*, 55–74.
39. IT Living Lab. (n.d.). Dostupno na: https://livlab.org/seta/ (Pristupljeno: 11. februara 2023.)
40. Jones, T. (2022). *The 12 Latest Types of Social Engineering Attacks (2023).* Aura. Dostupno na: https://www.aura.com/learn/types-of-social-engineering-attacks (Pristupljeno: 5. februara 2023.)
41. Jouini, M., Rabai, L.B. i Aissa, A.B. (2014) 'Classification of Security Threats in Information Systems', *Procedia Computer Science*, 32, pp. 489–496.

42. Junger, M., Montoya, L. i Overink, F.J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behaviour. 66*:75-87.
43. Kaushalya, T., Randeniya, R. i Liyanage, S. (2018). An Overview of Social Engineering in the Context of Information Security. *IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS),* 1-6.
44. Khonji, M., Iraqi, Y. i Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials, 15* (4), 2091–2121.
45. Knoke, D. (2005). Structural Equation Models. *Encyclopedia of Social Measurement.* Elsevier Inc. pp. 689-695.
46. Koyun, A. i Al Janabi, E. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST), 4*(6), pp. 7533-7538.
47. Krombholz, K., Hobel, H., Huber, M. i Weippl, E. (2015). Advanced Social Engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122.
48. Kumar, A., Chaudhary, M. i Kumar, N. (2015). Social Engineering Threats and Awareness: A Survey. *European Journal of Advances in Engineering and Technology, 2(11):* 15-19.
49. Liang, H. i Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71.
50. Lohani, S. (2019). Social Engineering: Hacking into Humans. *International Journal of Advanced Studies of Scientific Research, Vol. 4*, No. 1.
51. Malin, C.H., Gudaitis, T., Holt, T.J. i Kilger, M. *Deception in the Digital Age: Exploiting and Defending Human Targets through Computer-Mediated Communications,* 1st ed. Academic Press. Burlington, MA.
52. Mansour, R.F. (2016) "Understanding how big data leads to social networking vulnerability," *Computers in Human Behavior*, 57, pp. 348–351.
53. Mateos-Aparicio, G. (2011) 'Partial least squares (PLS) methods: Origins, evolution, and application to Social Sciences', *Communications in Statistics - Theory and Methods*, 40(13), pp. 2305–2317.
54. Merriam-Webster. (n.d.). *Security definition & meaning*. Merriam-Webster. Dostupno na: Pristupljeno 7. marta 2023. (Pristupljeno: 7. marta 2023.)
55. Microsoft Learn. (2023). *Personnel management overview - Microsoft Service Assurance*. Dostupno na: https://learn.microsoft.com/en-us/compliance/assurance/assurance-human-resources (Pristupljeno: 18. februara 2023.)
56. Microsoft Security. (2023). *Cybersecurity Awareness – Microsoft Security*. Dostupno na: https://www.microsoft.com/en-us/security/business/cybersecurity-awareness (Pristupljeno: 18. februara 2023.)
57. Microsoft. (2023). *Supplier Security & Privacy Assurance*. Dostupno na: https://www.microsoft.com/en-us/procurement/sspa (Pristupljeno: 18. februara 2023.)
58. Mitnick Security Consulting. (n.d.). The History of Social Engineering. Dostupno na: https://www.mitnicksecurity.com/the-history-of-social-engineering (Pristupljeno: 5. februara 2023.)
59. Mitnick, K. (2002). *The Art of Deception*. Indianapolis, Indiana: Wiley Publishing.
60. Mitnick, K. D. i Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, Indiana: Wiley Publishing.
61. Mohd Foozy, C. F., Rabiah, A., Mohd, A., Robiah, Y. i Masud, Z. (2011). Generic taxonomy of social engineering attack. *Malaysian Technical Universities International Conference on Engineering & Technology. 1-7.*
62. Mouton, F., Leenen, L. i Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209.

63. National Institute of Standards and Technology, N. I. (2003). *Building an Information Technology Security Awareness and Training Program: NiST SP 800-50.* Dostupno na: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf (Pristupljeno: 23. avgusta 2023.)
64. Nohlberg, M. (2005). Social Engineering Audits Using Anonymous Surveys: Conning the Users in Order to Know if They Can Be Conned. *Proceedings of the 4th Security Conferenc*e, Las Vegas, USA. Dostupno na: http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-1714 (Pristupljeno: 25. avgusta 2023.)
65. Odeh, N., Eleyan, D. i Eleyan, A. (2021). A Survey Of Social Engineering Attacks: Detection And Prevention Tools. *Journal of Theoretical and Applied Information Technology. 99 (18).*
66. Oles, N. (2023). 'Phishing Tactics and Techniques', *How to Catch a Phish*, pp. 23–31.
67. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. i Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.
68. Parthy, P. P., i Rajendran, G. (2019). Identification and prevention of social engineering attacks on an enterprise. *2019 International Carnahan Conference on Security Technology (ICCST)*.
69. Patel, N.J. (2021). *An Empirical Assessment of Users' Information Security Protection Behavior towards Social Engineering Breaches.* Doctoral dissertation. Nova Southeastern University. NSUWorks, College of Computing and Engineering. Dostupno na: https://nsuworks.nova.edu/gscis_etd/1157/ (Pristupljeno: 25. januara 2023.)
70. Posey, C., Roberts, T. L. i Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect Organizational Information Assets. *Journal of Management Information Systems*, *32*(4), 179–214.
71. Reid, R. i Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa*. https://doi.org/10.1109/issa.2014.6950492
72. Robinette, P., Li, W., Allen, R., Howard, A. M. i Wagner, A. R. (2016). Overtrust of robots in emergency evacuation scenarios. *11th ACM/*IEEE *International Conference on Human-Robot Interaction (HRI)*.
73. Rodriguez, R.M. i Atyabi, A. (2022). Social Engineering Attacks and Defenses in the Physical World vs. Cyberspace: A Contrast Study. *arXiv preprint arXiv:2203.04813*.
74. Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology (91:1).*
75. Salahdine, F. i Kaabouch, N. (2019). Social Engineering Attacks: A survey. *Future Internet, 11*(4), 89.
76. Saleem, J. i Hammoudeh, M. (2017). Defense methods against social engineering attacks. *Computer and Network Security Essentials*, 603–618.
77. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.K.R. i Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics, 9(9),* 1460.
78. Schaab, P., Beckers, K. i Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information & Computer Security*, *25*(2), 206–222.
79. Sethi, P. (2022). Social engineering in cyber security. *Jus Corpus Law Journal, 3(1),* 1025-1032.
80. Siddiqi, M. A., Pak, W. i Siddiqi, M. A. (2022, June 14). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences, 12*(12), 6042.
81. Smith, A., Papadaki, M. i Furnell, S. M. (2013). Improving Awareness of Social Engineering Attacks. *Information Assurance and Security Education and Training*, 249–256.

82. Sommestad, T., Karlzén, H. i Hallberg, J. (2015). A meta-analysis of studies on Protection Motivation Theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46.
83. Somun-Kapetanović, R. (2012). *Statistika u ekonomiji i menadžmentu.* Treće izdanje. Sarajevo: Ekonomski fakultet u Sarajevu.
84. Stamp, M. (2011). *Information security: Principles and practice.* John Wiley & Sons, Inc.
85. Stoica, A. (2021). Social Engineering as the new Deception Game. *Revista Română de Informatică și Automatică. 31*. 57-68.
86. Stroud, D. (2008). Social Networking: An age-neutral commodity — social networking becomes a mature web application. *Journal of Direct, Data and Digital Marketing Practice*, *9*(3), 278–292.
87. Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R. i Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access, 10*, 39325–39343.
88. Thomas, C., Fraga-Lamas, P. i Fernández-Caramés, T. (2020) *Computer security threats*. IntechOpen.
89. Verizon. (2022). *2022 Data Breach Investigations Report.* Verizon. Dostupno na: *https://www.verizon.com/business/resources/reports/dbir/* (Pristupljeno: 20. februara 2023.)
90. Vishwanath, A. (2014). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication*, *20*(1), 83–98.
91. Wang, Z., Sun, L. i Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access, vol. 8*, pp. 85094–85115.
92. Whitman, M. E. i Mattord, H. J. (2022). *Principles of Information Security*. Cengage.
93. Wilhelm, T. (2013). *Privilege Escalation. Professional Penetration Testing, 271–306.*
94. Wulandari, N., Adnan, M. S. i Wicaksono, C. B. (2022). Are You a Soft Target for Cyber Attack? Drivers of Susceptibility to Social Engineering-Based Cyber Attack (SECA): A Case Study of Mobile Messaging Application. *Human Behavior and Emerging Technologies*, 1–10.
95. Yasin, A., Fatima, R., Liu, L., Yasin, A. i Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. *Security and Privacy, 2(4*).
96. Yeboah-Boateng, E. O. i Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences, 5*(4), 6, 297-307.
97. Zulkurnain, A.U., Hamidy, A.K.B.K., Husain, A.B. and Chizari, H. (2015). Social Engineering Attack Mitigation. *International Journal of Mathematics and Computational Science, 1*, 188-198.

PRILOZI

Prilog 1. Anketa korištena u istraživanju

ANKETA: Socijalni inženjering kao prijetnja sigurnosti informacionih sistema

Poštovani/a,

Pred Vama je anketa čija je svrha prikupljanje podataka u svrhu naučnog istraživanja potrebnog za izradu master teze studentice Nataše Lizdek Kandić na drugom ciklusu studija Ekonomskog fakulteta Sarajevo na temu "Socijalni inženjering kao prijetnja sigurnosti informacionih sistema".

Anketa je namijenjena samo licima koja su zaposlena i imaju 18 ili više godina, a žive na teritoriji Bosne i Hercegovine.

Vaši odgovori u potpunosti su anonimni i neće se analizirati na pojedinačnom nivou, već zbirno, čime je zagarantovana Vaša privatnost. Učešćem ćete dati svoj doprinos za stvaranje relevantnih uvida i saznanja u oblasti informacione sigurnosti. Za odgovaranje će Vam biti potrebno 5-10 minuta vremena.

VAŽNO - Prije početka ankete molim Vas da pročitate sljedeće:

SOCIJALNI INŽENJERING - tehnika kojom se manipuliše ljudima tako da oni svjesno ili nesvjesno napadaču omoguće pristup njihovom računaru, što napadač koristi za neovlašteno pribavljanje podataka o korisniku i/ili njegovoj kompaniji

Primjeri socijalnog inženjeringa:

1. Neko Vam obećava besplatne stvari, kao što su telefoni, novčane nagrade i slično, a zauzvrat samo treba da se prijavite sa svojim korisničkim imenom i lozinkom na neku (lažnu) stranicu (ili da im uslikate i pošaljete svoju ličnu kartu)

2. Na računaru Vam se pojavljuje (lažno) upozorenje o virusima kojima je Vaš uređaj zaražen (cilj je da kliknete na link i time nesvjesno instalirate zlonamjerni softver koji zatim tajno prikuplja podatke o Vama ili zahtijeva da platite da Vas oslobode virusa kojima ste zaraženi)

3. Neko Vam šalje e-poštu u kojoj se (lažno) predstavlja kao Vaš šef ili poslovni kolega i hitno Vam traži određene podatke

---

S poštovanjem,

Nataša Lizdek Kandić, student drugog ciklusa studija Ekonomskog fakulteta Sarajevo

Filter pitanja

1. **Da li živite na teritoriji Bosne i Hercegovine? (**Izaberite jedan od ponuđenih odgovora.)

   - Da
   - Ne

2. **Da li ste trenutno zaposleni?** (Izaberite jedan od ponuđenih odgovora.)

   - Da
   - Ne

Demografski podaci

1. Koji je Vaš pol? (Izaberite jedan od ponuđenih odgovora.)

- Muški
- Ženski

2. Koji je Vaš nivo obrazovanja? (Izaberite jedan od ponuđenih odgovora.)

- SSS
- VŠS
- VSS
- MA ili MR
- DR

3. Kojoj industriji pripada kompanija/institucija u kojoj ste zaposleni? (Izaberite jedan od ponuđenih odgovora.)

- IT
- Finansije i/ili računovodstvo
- Marketing i slične usluge
- Proizvodnja
- Obrazovanje
- Ostalo

4. **Koliko imate godina?** (Izaberite jedan od ponuđenih odgovora.)

- od 18 do 25
- od 26 do 35
- od 36 do 45
- od 46 do 55
- od 56 do 65

5. **Koja je vaša pozicija u kompaniji?** (Izaberite jedan od ponuđenih odgovora.)

- Radnik na operativnom nivou
- Šef odjela
- Srednji menadžment
- Top menadžment

6. Koliko iskustva imate u korištenju računara? (Izaberite jedan od ponuđenih odgovora.)

- manje od 1 godine
- između 1 i 3 godine
- između 3 i 6 godina
- između 6 i 10 godina
- više od 10 godina

7. Koliko ste do sad bili izloženi računarskim napadima socijalnim inženjeringom (npr. da ste dobili lažnu poruku ili e-poštu kojima je neko pokušao da Vas prevari tako što se lažno predstavio i zatražio od Vas neke lične informacije)? (Izaberite jedan od ponuđenih odgovora.)

- Nimalo
- Donekle
- Izrazito

Percipirana ozbiljnost (PO)

Ocijenite koliko se slažete sa narednim tvrdnjama.

PO01 Ako bih doživio ugroženost informacione sigurnosti usljed upada socijalnim inženjeringom pretrpio bih mnogo tegoba.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PO02 Ako bih doživio ugroženost informacione sigurnosti usljed upada socijalnim inženjeringom to bi bilo užasno.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PO03 Ako bih doživio ugroženost informacione sigurnosti usljed upada socijalnim inženjeringom shvatio bih to ozbiljno.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PO04 Ako bih izgubio podatke usljed upada socijalnim inženjeringom to bi bio značajan događaj u mom životu.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PO05 Uništenje mojih podataka usljed upada socijalnim inženjeringom bio bi ozbiljan problem za mene.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

Percipirana ranjivost (PR)

Ocijenite koliko se slažete sa narednim tvrdnjama.

PR01 Vjerovatno ću doživjeti ugrožavanje informacione sigurnosti usljed upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PR02 Velike su šanse da ću izgubiti povjerljive podatke u budućnosti usljed upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PR03 Postoji mogućnost da su moji lični podaci procurili usljed upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PR04 Moji podaci će vjerovatno biti ugroženi zlonamjernim softverima kao što su virusi tokom upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

PR05 Moj sistem će vjerovatno biti oštećen upadom socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

Strah (ST)

Ocijenite koliko se slažete sa narednim tvrdnjama.

ST01 Brinem se zbog mogućnosti ugrožavanja informacione sigurnosti upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ST02 Osjećam strah zbog mogućnosti ugrožavanja informacione sigurnosti usljed upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ST03 Osjećam tjeskobu zbog mogućnosti ugrožavanja informacione sigurnosti usljed upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ST04 Bojim se mogućnosti ugrožavanja informacione sigurnosti usljed upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ST05 Moj računar bi mogao postati neupotrebljiv zbog ugrožavanja informacione sigurnosti usljed upada socijalnim inženjeringom.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

Motivacija za zaštitu (MZ)

MZ01 Namjeravam da se pridržavam mjera za zaštitu informacione sigurnosti kako bih spriječio napade socijalnim inženjeringom u naredna 3 mjeseca.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

MZ02 Predviđam da ću se pridržavati mjera za zaštitu informacione sigurnosti kako bih spriječio napade socijalnim inženjeringom u naredna 3 mjeseca.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

MZ03 Planiram se pridržavati mjera za zaštitu informacione sigurnosti kako bih spriječio napade socijalnim inženjeringom u naredna 3 mjeseca.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

MZ04 Preduzimaću mjere predostrožnosti protiv kršenja informacione sigurnosti u naredna 3 mjeseca.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

MZ05 Neću instalirati nepouzdan softver na moj računar u naredna 3 mjeseca.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

Zaštitno ponašanje (ZP)

ZP01 Povremeno provjeravam i odstranjujem viruse i zlonamjerni softver.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ZP02 Odmah brišem sumnjive mejlove bez da ih pročitam.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ZP03 Ni pod kakvim uslovima ne bih s drugima podijelio svoj ID, lozinku ili druge kredencijale.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ZP04 Osiguravam primjenu najnovijih alata i tehnologija na mom računaru u skladu sa preporučenim mjerama informacione sigurnosti.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

ZP05 Ne nastavljam sa izvršenjem bilo koje aktivnosti za koju posumnjam da bi mogla izazvati upad socijalnim inženjeringom (npr. korištenjem nesigurne internet konekcije).

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

Obuka zaposlenih (OZ)

OZ01 Moja organizacija/poslodavac pruža trening kako bi pomogla zaposlenima da poboljšaju svijest o računarskim i informacionim sigurnosnim problemima.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

OZ02 Moja organizacija/poslodavac edukuje zaposlene o odgovarajućoj upotrebi IT resursa.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

OZ03 Moja organizacija/poslodavac informiše zaposlene o posljedicama neodobrenih izmjena računarskih podataka.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

OZ04 Moja organizacija/poslodavac trenira zaposlene u vezi sa njihovim odgovornostima za računarsku sigurnost.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem

OZ05 Moja organizacija/poslodavac edukuje zaposlene o njihovim odgovornostima pri upravljanju lozinkama na računaru.

- Uopšte se ne slažem
- Ne slažem se
- Donekle se ne slažem
- Niti se slažem, niti ne slažem
- Donekle se slažem
- Slažem se
- Potpuno se slažem